Copyright © 2005, Nortel Networks Nortel Networks Confidential

Upgrading the Gateway Controller

What's new for SN08

The following features or notable changes affect gateway controller (GWC) upgrades for the SN08 release:

- A00007100 - MCP905 Next Generation GWC Card.
  Introduction of the MCPN905 GWC card to replace the MCPN750 card (optional).
- A00007140 - Upgrade Manager Phase 1.
  Introduction of the GWC Upgrade Tool, which upgrades selected GWCs and applies patches automatically.
- A00007564 - SAM21 EM Support for New Hardware MCPN905.
- A00007927 - SAM21 EM Enhancements from Bell Canada VO.
- Q00834467 - Introduction of the Get Load Files button and the drop-down menu (to select a load).
- Restructured introductory sections:
  - The next section, Prepare to upgrade the gateway controller on page 13still contains general information (such as service impact) that the user should be aware of before carrying out an upgrade.
  - Then a new section Overall GWC upgrade process - automated on page 19 outlines the new automated upgrade process.
  - This is followed by the detailed new procedure Upgrade the GWC using the GWC Upgrade Tool on page 23.
  - The document also contains the original section Overall upgrade process - manual on page 65 and its associated manual procedures for use if necessary.

- PVG naming - The table below lists the names used for certain gateways in Carrier VoIP documentation prior to SN07, and provides the new brand names starting in SN07.

Pre-SN07 name	New brand name (starting in SN07, implemented for GWC in SN08)
Passport Packet Voice Gateway (PVG)	Nortel Media Gateway 7480 or 15000
PVG 7400 or PVG 7K	Nortel Media Gateway 7480
PVG 15000 or PVG 15K	Nortel Media Gateway 15000
Note: The CS 2000 GWC Manager does not reflect these branding changes in SN08. As a result, neither does the GWC customer documentation reflect the changes. This table is provided to map the names used in GWC documentation to other Carrier VoIP documentation	

Upgrade strategy

There are no direct software upgrades for the GWC. Instead GWC software upgrades are supplied to the GWC image loaded on the CS 2000 Management Tools server.

Upgrading the GWC occurs when a new software load image is delivered to the customer site. Read the entire GWC upgrades Overview section of this document thoroughly to learn the different types of upgrades and conditions applied to each upgrade.

Additionally, GWC software updates may be incrementally delivered through a GWC software patches. GWC patches are applied according to the release specifications for the patch. GWC software patches are released and applied to the GWC image files using the Network Patch Manager (NPM), an application in the CS 2000 Management Tools suite. The release specifications can be found by running a patch list report using the NPM **Tasks|Reports** menu. Some patches are applied only after other patches have been removed. Other patches are applied only under special circumstances. Patches can be applied during an upgrade or on their own as corrective content.

Upgrade process

You can upgrade the GWC using one of the following methods:

- Automated process - This is the recommended method. It uses the GWC Upgrade Tool, which performs all necessary actions in a specific sequence by invoking the functions of the CS 2000 GWC

Manager, CS 2000 SAM21 Manager, and Network Patch Manager. Refer to section Overall GWC upgrade process - automated on page 19.

- Manual process - This involves completing a set of manual procedures in a specific sequence on several network components. Refer to section Overall upgrade process - manual on page 65.

Downgrade process

If you need to roll back a software upgrade and revert to a previous software load, refer to one of the following procedures:

- Automated process - Downgrade procedure on page 60.
- Manual process - Roll back a software upgrade on a GWC node on page 107.

Hardware upgrade

If you need to upgrade the GWC hardware, replacing the MCPN750 cards with MCPN905 cards, refer to procedure Upgrade a GWC node's hardware - MCPN750 to MCPN905 on page 149.

Software delivery methods

Upgrade loads are delivered using one of the following delivery methods:

- CD-ROM
- Electronic Software Delivery (ESD)

Delivered load are installed on the CS 2000 Core Manager or Core and Billing Manager. Any patch files delivered along with the upgrade load are delivered on CD-ROM and installed on the NPM server. Patches may be included in the load image. To view any patches that are available with the load image, refer to procedure View the contents of a load file image on page 87. If you want to see what patches are inside the load file, you must still retrieve patch files so that NPM has the ability to remove the imaged patches.

Note: Starting in SN06, Network Patch Manager implements new login authorization policies. Refer to the CS 2000 Management Tools section in *ATM/IP Solution-level Configuration Management*, NN10409-500, to ensure that NPM is properly configured so that you can log onto the NPM GUI or CLUI to perform patching activities.

Software patches can also be delivered using electronic software delivery (ESD). For more information on delivering patches, refer to section Patch file acquisition on page 5.

Necessary procedures or checklists used to complete this process are found in “Carrier Voice over IP Network patching” section of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site’s ESD is implemented, contact your site network administrator. Also, refer to *Upgrading a Carrier Voice over IP Network*, NN10440-450 and *Electronic Software Delivery Customer Implementation Guide*, NE10003-112.

Tools and utilities

A GWC manual software upgrade requires the CS 2000 SAM21 Manager client interface.

The GWC upgrade tool, introduced with the SN08 release, is distributed with the CS 2000 Management Tools software package. This tool also requires that the CS 2000 SAM21 Manager and the NPM are upgraded, configured, and functioning with the SN08 software load.

NPM is an application in the CS 2000 Management Tools suite. It is used to install a patch into GWC software. This patched load image is optionally saved back to the software load location on the CS 2000 Core Manager or CBM and is available to other GWCs when they reboot. A patched load is saved through the CS 2000 GWC Manager interface. For more information about configuring NPM, refer to the CS 2000 Management Tools section in *ATM/IP Solution-level Configuration Management*, NN10409-500. For more information about using NPM, refer to the “Carrier Voice over IP Network patching” section in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (Integrated EMS). In addition, access to the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, is now provided using the Integrated EMS. For more information, refer to *Integrated EMS Basics*, NN10329-111.

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in *Integrated EMS Basics*, NN10329-111:

- "Launch GWC Manager"
- "Launch SAM21 Manager"

Troubleshooting upgrade problems

Should any problems occur during upgrade, or rollback (downgrade) activities, refer to procedure Troubleshoot GWC upgrades on page 141 for assistance.

Patching procedures

Patching activities occur when new patches become available and need to be installed and activated. They also occur when an older patch becomes obsolete and must be deactivated and/or removed. For more information about patching activities refer to the "Carrier Voice over IP Network patching" section in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Although most patch files apply to any Nortel Networks customer site, some patch files are created for a particular customer's site-specific GWC changes. Not all patches made available apply to all customer sites. Apply all patches to the GWC, including activatable (ACT) patches that apply to your site. Contact Nortel Networks customer support to determine which activatable patches are to be activated in your site. Do not activate any other GWC ACT category patches unless advised to do so by Nortel Networks customer support.

Patch file acquisition

Patch files can be released either at upgrade time or in between upgrades. When patch files are made available during upgrade activity, they are sent on a separate CD-ROM delivered with the new software load. When patch files become available in between upgrade periods, they are delivered by way of Electronic Software Delivery (ESD) to the server supporting your CS 2000 Management Tools software using one of the following methods.

- Drop box - patch files are pushed from Nortel Networks to an external drop box location. The drop box can exist on the Nortel Networks Customer Access Network (CAN), or the customer's wide area network (WAN).
- Web distribution - patches are pulled through the Internet from a secure Nortel Networks web page and stored on a customer-provided server. Web distribution is done through www.nortelnetworks.com. Patches are located under Support &

Training -> Software Downloads -> (Browse Product Support tab) 1 Product Families: Succession or Succession Communication Server 2000 -> 2 Product menu: Communication Server 2000 -> 3 Content menu: Software.

Note: Use the filter criteria to display only a selected set of patches.

Also, to facilitate patch management, the following two tools are available under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Tools:

- Pre Upgrade Patch Calculator - use it to identify patches that have been released against your CD-ROM after it has been shipped.
- Patch Audit for Inform List - use it to perform site-specific audit to identify any missing patches.

Note: For instructions on how to use each of these tools, refer to the Readme file that can be found under each corresponding link.

Patch activation

Once a patch has been received into the NPM database, a patch can be activated if:

- the patch is not on hold
- the patch has a category of ACT
- the patch has been applied to a GWC card
- the device is not on hold

Patch deactivation

A patch can be deactivated from the NPM if:

- the patch has been activated previously
- the patch is not on hold
- the device is not on hold
- the patch has a category of ACT

Patch replacement

If an ACT patch happens to become obsolete, a new patch file with the same patchid containing a category of OBS (obsolete) or OBE (obsolete emergency) is sent to the office.

The new obsolete patch replaces the original patch file in the NPM database once the following activities occur in the following order:

- first, the ACT patch has been deactivated and removed from all devices
- next, the patch has been retrieved using the NPM getpatch command.

Once the OBS or OBE category patch has replaced the original ACT category patch; the patch can NO longer be activated.

The NPM currently sets a major alarm for OBS category patches that are applied and a critical alarm for OBE patches that are applied.

Note: This feature does not change the overall principle of how patch file replacement occurs in the NPM, except that if the patch is activated it must first be deactivated. A patch file can be replaced only while the patch is applied and/or activated if the code section of the patch has not changed.

Patch removal

To use the patch removal command ensure that a patch has been deactivated before attempting to remove it from the patched device. The patch remains in the NPM database.

NPM CLUI User authentication for patching activities

Starting in SN06, NPM CLUI authentication is implemented by a new login method which prompts for a user ID and password, then interacts with the SSPFS servlet application on the CS 2000 Management Tools server for authentication. For more information about user authentication and the NPM CLUI, refer to the CS 2000 Management Tools section in *ATM/IP Solution-level Security and Administration*, NN10402-600.

GWC software imaging

An image of a GWC software load, including all patches, can be taken from a GWC device and saved on the CS 2000 Core Manager or CBM to act as a load file. When they are rebooted, GWC devices managed by the CS 2000 Core Manager or CBM receive the load file, if they are provisioned to do so.

There are two ways to take an image of a GWC software load:

- You can take a manual image of a load. For this procedure, refer to Take a manual GWC software image on page 119
- You can enable the CS 2000 GWC Manager to automatically save a new image of a software load on the CS 2000 Core Manager or

CBM once daily, if required. For this procedure, refer to Enable or disable GWC software auto-imaging on page 137

Note: You may also receive a load image, with or without patches, from Nortel Networks.

Nortel Networks recommends that you apply all Released (R) and Propagated (P) status patches, take the image, and then apply Verification (V) status patches. It is best not to have V status patches in a saved image since these patches are normally applied to only one GWC.

When enabled, auto-imaging executes once daily at 2:00 AM. You cannot schedule auto-imaging to occur at a different frequency or at a different time.

Auto-imaging - patch criteria

When auto-imaging is enabled, the CS 2000 GWC Manager (GWC Manager) uses information from the NPM to determine if it needs to take an image of a software load. The GWC Manager then determines which GWC devices would be good candidates.

All GWC devices running a particular software load are examined. A device is considered a candidate for imaging if it has the following characteristics:

- It contains a software load with the highest application level. Load application level is considered first.
- It contains a software load with the highest activation level. Load activation level is considered after application level.
- It is not on hold. (When a device is on hold, no patching or auto-imaging can occur.)

If two or more GWC devices contain the highest application level of the same software load, the devices that contain the highest patch activation level are sent to the GWC Manager as candidates for imaging. If the activation levels are equal among all devices, then all devices are sent to the GWC Manager as candidates.

The following tables show an example of how the application and activation levels are used to determine which GWC devices can be sent to the GWC Manager as candidates for imaging.

All GWC devices available for two software loads and their status

Software load	Device	AppLevel	ActLevel	On hold?
A				
	GWC 1	5	0	N
	GWC 2	5	1	N
	GWC 3	6	0	N
B				
	GWC 4	3	3	N
	GWC 5	3	3	N
	GWC 6	3	2	N
	GWC 7	5	0	Y
	GWC 8	3	3	N

Candidate devices for each load

Software load	Candidate devices
A	
	GWC 3
B	
	GWC 4
	GWC 5
	GWC 8

Compare the table listing the candidate devices for each load with the table showing all GWC devices available.

Software load A contains only one GWC candidate device, GWC 3. This device is chosen because it has the highest application level.

Although GWC 2 has a patch that has been activated, it is not chosen because its application level is not as high as GWC 3.

Software load B contains three candidate devices, GWC 4, GWC 5 and GWC 8. Although GWC 7 contains the highest patch activation level, it has been manually placed on hold. Although GWC 6 has an application level of 3, the activation level of this device is lower then the activation levels of GWC 4, GWC 5 and GWC 8.

Auto-imaging - CS 2000 GWC Manager criteria

When the list of candidate loads is provided by the NPM, the CS 2000 GWC Manager (GWC Manager) uses its own criteria to determine which device to image. This criteria is based on the activity state of each device in the candidate list for a software load. The GWC Manager takes an image of the first inactive or locked device in the candidate list for a load. If all devices in the candidate list are active, the GWC Manager selects the first device in the list.

The following table illustrates the criteria that the GWC Manager uses to choose a device for to image from the candidate list.

Devices selected for imaging by the CS 2000 GWC Manager

Software load	Device selected (*)	Active?
A		
	*GWC 3	Y
B		
	*GWC 4	N
	GWC 5	Y
	GWC 8	N

For software load A, although GWC 3 is active, it is the only device in the candidate list using that load.Therefore, the GWC Manager takes an image of GWC 3.

For software load B, the GWC 4 is the first inactive device in the list. Therefore, the GWC Manager takes an image of GWC 4.

Considerations for using auto-imaging

Auto-imaging is an effective tool when you want to be certain that a new image of a GWC device is saved to the CS 2000 Core Manager or CBM

after the device is patched. It is useful in an office where you apply and activate the same patches to all GWCs with the same load.

- Auto-imaging is not designed for an office in which different patches are applied to GWCs using the same software load.
- If you take a manual image, there is no guarantee that a load has been patched and that taking a new image is necessary. Also, after the load file has been manually replaced on the CS 2000 Core Manager or CBM, there is no way of knowing if it is the original load file or the newly imaged load file. The name of the load file does not change.
- If you take only manual images you risk losing a patch application if you neglect to take an image after patching a software load. If you have auto-imaging enabled, you may still need to take manual images to execute upgrade procedures in this document.
- You can use both auto-imaging and manual-imaging. You can keep auto-imaging enabled and take manual images, as well.

Managing firmware on GWC cards

The following procedures allow you to ensure that you have the latest firmware version for GWC cards in your system and that any problems with your GWC firmware are resolved:

- To upgrade the version of firmware on GWC cards in your system, refer to procedure Firmware flash a GWC card on page 123.
- To resolve problems with the firmware on a GWC card, refer to procedure Force a firmware flash of a GWC card on page 129.

Prepare to upgrade the gateway controller

This section provides details on specific items that users must be aware of prior to upgrading gateway controller (GWC) nodes in a CS 2000.

Ensure that you research each item in the GWC upgrade preparation list in the following table.

GWC upgrade preparation list

Item	√	Details
Upgrade paths supported		Depends on your solution. See the supported upgrade paths in the SN08 upgrade document, *Upgrading a Carrier Voice over IP Network*, NN10440-450.
Upgrade order for all GWC card types		Applicable to all solutions. See section Upgrade order for all GWC card types on page 13.
Upgrade and downgrade call service impact		Applicable to all solutions. See Upgrade and downgrade call service impact on page 16.
Ensure compliant characters in RMGC application domain name		Applicable to IP solutions (Integrated Access Wireline, Cable, IP). See Ensuring compliant characters in RMGC application domain name on page 16.
Allocate time for a GWC upgrade		Applicable to all solutions. See Allocating time for a GWC upgrade on page 17.
Impact of an upgrade on GWC configuration		Applicable to all solutions. See Impact of an upgrade on GWC configuration on page 17.

Upgrade order for all GWC card types

All GWC cards of the same type must be upgraded before moving on to the next group. For example, all audio controller GWC cards must be

upgraded before upgrading the next GWC card-type present in your system. The new GWC Upgrade Tool automatically upgrades the card types in the correct order.

The order presented includes all GWC card types, even though some of the card types indicated cannot co-exist in the same installation. For the GWC card type order specific to your solution, refer to *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Upgrade GWC card pairs from SN06.2 or SN07 to SN08 in the following order of card type:

Note: For definitions of the terminology in the list, refer to the Glossary of terms in *Gateway Controller Basics*, NN10189-111.

GWC card type upgrade order

Order	GWC card type
1	AC
2	BICC - UA-AAL1 solutions only
3	VRDN
4	Session Server (SN07 to SN07, SN07 to SN08 and SN08 to SN08 upgrades only) - see Note 1
5	SIP-T/APG/RA - see Note 2
6	APG/RA - see Note 2
7	SIP-T/APG - see Note 2
8	APG - see Note 2
9	SIP-T
10	Trunk
11	H.323
12	V5.2 trunk
13	Lines - includes CICM

Note 1: The Session Server (SS) was a new component in SN07. It can replace the Virtual Routing Destination Node (VRDN) GWC as a SIP-T interface. The following office configurations are supported in

SN07: SS only, VRDN SIP-T only, or VRDN SIP-T and SS co-existing in the same office. For the upgrade order specific to your solution, refer to *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Note 2: The APG functionality was removed in the SN07 release. All GWC service profiles and gateway profiles that were required to support the APG functionality (all profiles with “APG” in their names, such as, SIP_T_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. It is recommended that the existing DPT GWCs that still use these profiles migrate to SIP-T or SIP_TINTL profile to optimize resource utilization (resources previously reserved for APG are released for other tasks). The Packet Media Anchor (in IP network solutions) is the replacement device for the APG functionality.

Note 3: The manual upgrade process does not support parallel upgrades. While it is possible to save time by loading all GWC card pairs of a given GWC type and performing all the SwActs at the same time, this is not recommended or supported for a live office upgrade as it would cause an out of service condition for all GWC nodes.

Note 4: Starting in SN06, the Redirecting Media Gateway Controller (RMGC) application migrates from the CS 2000 Management Tools server to the GWC platform. RMGC service cannot be provided between upgrading the CS 2000 Management Tools server and commissioning the GWC-based RMGC service. Refer to *Upgrading a Carrier Voice over IP Network*, NN10440-450 for a complete migration strategy for this feature.

It is assumed that an existing Audio Controller GWC is used to host the RMGC application. If commissioning a new GWC for RMGC in SN08, refer to appropriate procedures in *Gateway Controller Configuration Management*, NN10205-511.

Upgrade and downgrade call service impact

The following matrix shows expected service impact for the GWC card types over the supported GWC load change scenarios.

Upgrade and downgrade call service impact

GWC type	SN06.2/07 -> SN08 Upgrade	SN08 -> SN08 Maintenance (patching)	SN08 -> SN07 Downgrade	SN08 -> SN06.2 Downgrade
AUDCNTL	Stable announcement and conference calls survive.	Stable announcement and conference calls survive.	Stable announcement and conference calls survive.	Stable announcement and conference calls.
VRDN	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	ALL calls survive.	ALL calls survive.
SIP-T	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	NO calls survive.	NO calls survive.
MG 15000 Trunk	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	SOME calls may survive.	NO calls survive.
APG	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	SIP-T calls using an APG do not survive.	SIP-T calls using an APG do not survive.
Line or H.323	Stable 2-party calls survive. Possible limited functionality after the swact. For SN07 to SN08 upgrade, H.323 gateway calls survive (except Cisco gateway). For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable.	Stable 2-party calls survive. Possible limited functionality after the swact. For unstable dialing, ringing, clearing or multi-party calls the behavior is unpredictable.	SOME calls may survive. H.323 gateway calls survive (except Cisco gateway). Billing records may not be produced when calls go on-hook.	SOME calls may survive. Billing records may not be produced when calls go on-hook. H.323 gateway-based calls do not survive.

Note: This table omits the SN06 to SN08 upgrade/downgrade, which is supported for AAL1 solutions only. The AAL1 solution does not include GWC.

Ensuring compliant characters in RMGC application domain name

If you are upgrading to SN08 and intend to use the Redirecting Media Gateway Controller (RMGC) application, you must be aware that using

invalid or non-RFC 1034 compliant characters (such as the underscore character) for the GWC domain name in the GWC database could render the RMGC application unusable. Check the cmshortCLLIname, which is datafilled in table OFCENG as office parameter OFFICE_CLLI_NAME in the XA-Core, before the upgrade begins to determine if it uses any characters that are not compliant with RFC 1034. Correct this value before the upgrades are started on the XA-Core. Refer to your applicable *Office Parameter Reference Manual*, NTP 297-8001-855 or NTP 297-9051-855, to perform this task.

Consult your site system administrator for assistance in determining the domain name for your site. If you are commissioning a new GWC for RMGC in SN08, refer to procedures in *Gateway Controller Configuration Management*, NN10205-511.

Allocating time for a GWC upgrade

The time required for an average upgrade is 24 minutes for each GWC node (card pair) for the GWC software. Under a moderately loaded 10BaseT network, the load takes about 2 minutes to transfer. Transfer time can increase over a heavily loaded network.

The following time factors apply to tasks in the GWC upgrade activity.

- Total upgrade time for each GWC pair is 24 minutes (12 minutes for each card).
- Time needed to apply the GWC load package to CS 2000 Core Manager or CBM is 5 minutes.
- Time to perform a GWC node warm SWACT is 1 minute.
- Time to carry out the post upgrade call processing check for each GWC node is 2 minutes.
- The total upgrade time for all GWCs depends on the upgrade mode used in the GWC Upgrade Tool (see section Configurable options on page 26 of procedure Upgrade the GWC using the GWC Upgrade Tool) and the number of different GWC card types.

Impact of an upgrade on GWC configuration

Once the CS 2000 Core Manager or CBM is upgraded, you cannot provision GWCs until the CS 2000 Management software package is upgraded and configured on the CS 2000 Management Tools server.

Overall GWC upgrade process - automated

This section outlines the new automated process using the GWC Upgrade Tool for upgrading selected GWCs and applying patches.

Note 1: Starting in SN08, the automated process is the recommended process for upgrading the GWC. However, if you wish to use the original manual process, refer to procedure Overall GWC upgrade process - manual in *Upgrading the Gateway Controller*, NN10196-461.

Note 2: Before you begin, make sure that you have researched and addressed all the preparatory items described in procedure Prepare to upgrade the gateway controller in *Upgrading the Gateway Controller*, NN10196-461.

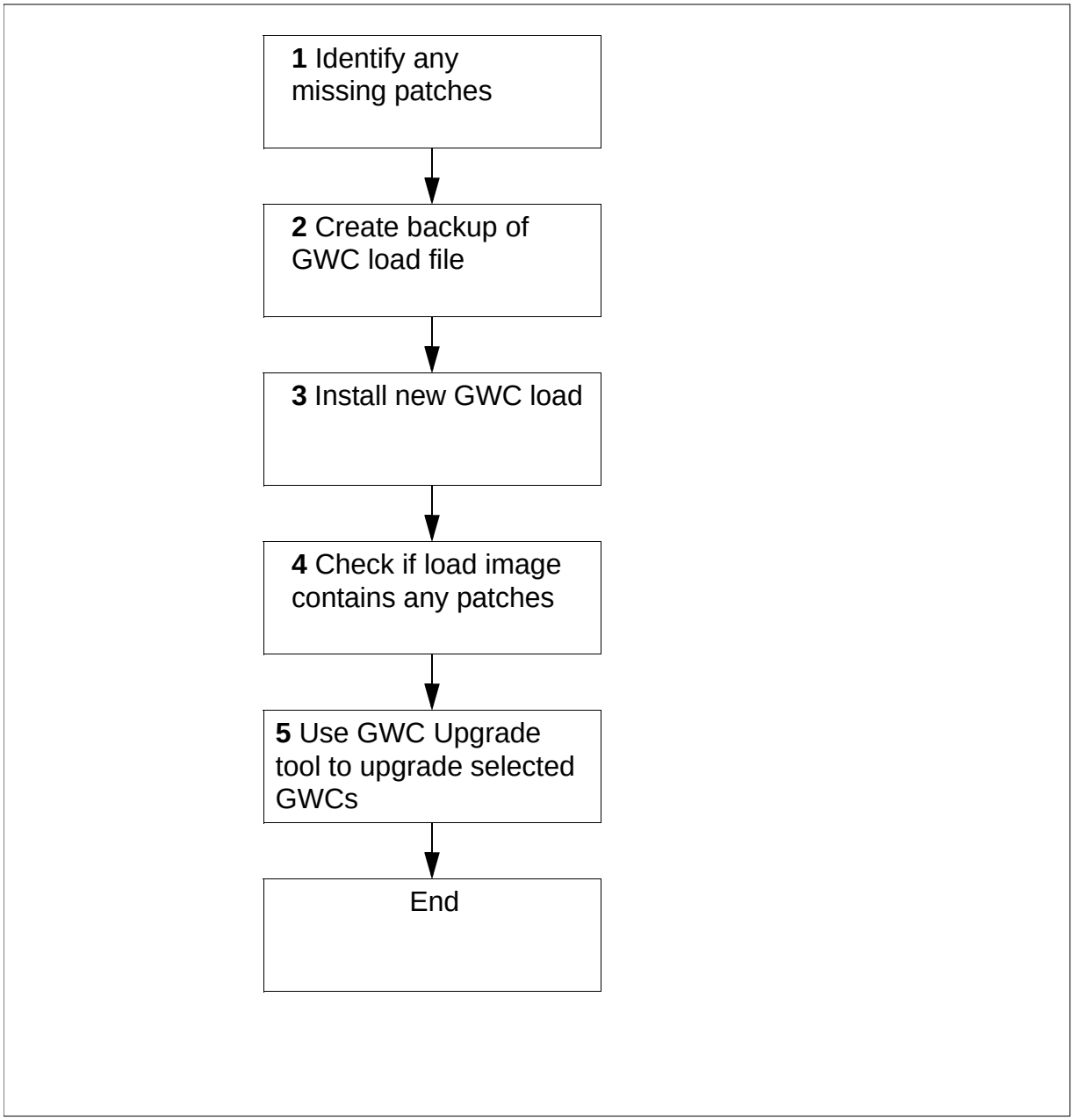
ATTENTION

For IP network solutions only (starting in SN07), the call agent identifier (ID) must be set for the CS 2000. This should typically be done prior to upgrading the GWC cards. For details, refer to section “CS 2000 call agent identifier” in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Summary flowchart

The following flowchart summarizes the overall GWC upgrade process. The numbers relate to the steps of the detailed procedure in section Overall GWC upgrade procedure on page 21 following the flowchart.

Summary of the overall GWC upgrade procedure



Overall GWC upgrade procedure

1 If necessary, complete the sub-steps (a) and (b) using one of the tools available at www.nortelnetworks.com.

Note: These steps may not be needed if you have obtained the soaked load from Nortel Networks GNPS (with all the necessary patches applied).

To obtain the tools:

- Under Support & Training, select Software Downloads.
- Select the Browse Product Support tab (this is usually the default choice).
- Follow the three steps displayed on the page:
  Step 1 - Product Families: select Succession or Succession Communication Server 2000.
  Step 2 - Product menu: select Communication Server 2000.
  Step 3 - Content menu: select Tools, then press 'Go'.
- For instructions on how to use each tool, refer to the Readme file that can be found under each corresponding link.

a Identify patches that have been released against your CD-ROM after it has been shipped - use the tool Pre Upgrade Patch Calculator. Download these patches (if any) to the site and retrieve the patch files for the NPM to process using the NPM CLUI **getpatch** command.

b Perform a site-specific audit to identify any missing patches - use the tool Patch Audit.

2 For security, back up your existing software load using procedure Create a backup of the GWC load file on page 85.

3 Install the new load using one of the following methods:

- from CD-ROM - use procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 69 in *Upgrading the Gateway Controller*, NN10196-461
- using ESD - use procedure Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 75 in *Upgrading the Gateway Controller*, NN10196-461

4 Check whether the load image contains any patches using procedure View the contents of a load file image on page 87. If so, add the patches to NPM as described in step 1a.

5 Upgrade the GWCs:

a If a day or more has passed between completing step 1a and performing the upgrade, repeat step 1b, then continue to step 5b.

b Use the GWC Upgrade Tool to upgrade the GWCs. Refer to procedure Upgrade the GWC using the GWC Upgrade Tool on page 23. The tool upgrades all selected GWCs to the given new load, and applies all available patches in NPM.

Note: Nortel Networks recommends that you apply all patches with status Released (R) and Propagated (P), take the image, and then apply the patches with status Verification (V). The GWC Upgrade Tool attempts to apply all available patches to all the GWCs. It is preferable not to have V status patches in a saved image, as these patches are normally applied to only one GWC.

If V status patches are found during the upgrade process, the GWC Upgrade Tool pauses to allow you to apply these patches manually.

GWC Upgrade Tool

The Main Menu contains all the options necessary for configuring and performing the automated GWC upgrade process.

```
Main Menu for GWC upgrade tool
1 -  Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Upgrade the GWC using the GWC Upgrade Tool

Purpose of this procedure

This procedure describes how to upgrade the software load from which the GWC cards boot, located on the CS 2000 Core Manager or Core and Billing Manager (CBM).

When to use this procedure

Use this procedure after installing a newer version of the GWC software load onto CS 2000 Core Manager or CBM. This procedure upgrades all selected GWC nodes installed in the SAM21 shelf that is being upgraded.

Prerequisites and guidelines

CAUTION

No provisioning activity can occur on the system while the GWC software upgrade is in progress.

The GWC software load filesets must be installed on CS 2000 Core Manager or CBM. Refer to one of the following procedures:

- Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 69 in *Upgrading the Gateway Controller*, NN10196-461
- Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 75 in *Upgrading the Gateway Controller*, NN10196-461

All the necessary patches must be loaded into NPM. Refer to procedure Overall GWC upgrade process - automated (step 1 on page 21).

The NPM automated processes must be disabled. Refer to step 29 of this procedure.

If the Communication Server LAN (CS LAN) is provided by Nortel Networks Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to “auto-negotiate”. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the GWC Upgrade Tool. Refer to procedure Re-provision the Ethernet Routing Switch 8600 port to auto-negotiate on page 62.

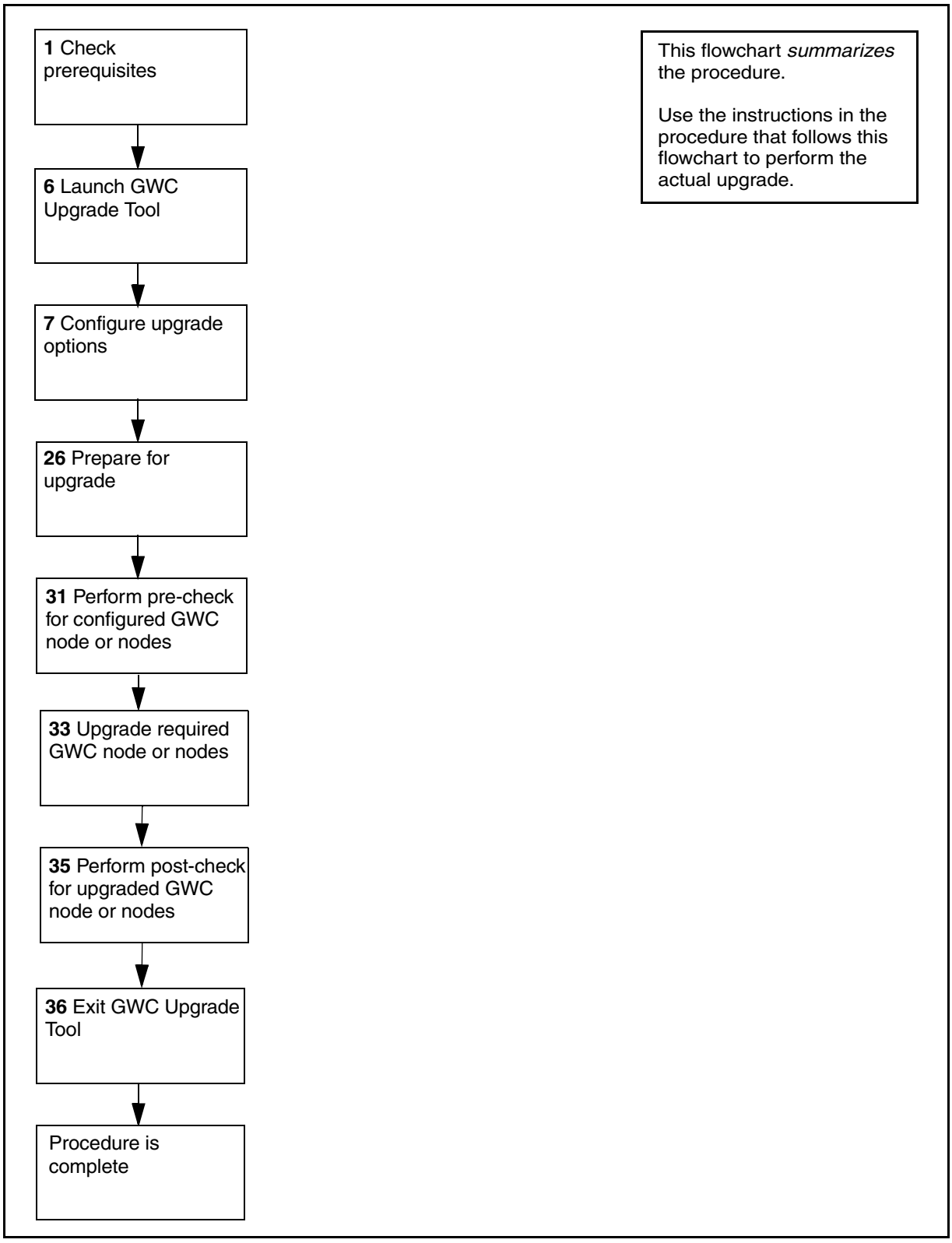
Overview

The GWC Upgrade Tool is distributed with the CS 2000 SESM package. The tool supports GWC upgrades via a command line user interface (CLUI). The tool is recommended as an alternative to the manual procedures (see procedure Upgrade a standby GWC card software load in *Upgrading the Gateway Controller*, NN10196-461), and automatically performs the following GWC upgrade operations:

- locks the inactive unit of the first selected GWC node (‘seed’ node), provisions it with a new load, and unlocks the unit
- busies the upgraded inactive unit, carries out a device audit, applies all available patches, returns the unit to service and swacts the ‘seed’ node
- locks the newly inactive unit of the ‘seed’ node, provisions it with the new soaked load, and unlocks the unit
- for all the other selected GWC nodes in turn (‘non-seed’ nodes) locks the inactive unit, provisions it with the new soaked load, unlocks the unit, and swacts the node
- locks the newly inactive unit of the ‘non-seed’ node, provisions it with the new soaked load, and unlocks the unit

The following flowchart provides an overview of the automated upgrade procedure. The numbers relate to the steps of the procedure in section Upgrade procedure on page 29 following the flowchart.

Automatic upgrade overview



Configurable options

The user can configure 11 options in the GWC Upgrade Tool. Two options are mandatory, and one of them must be given a specific value. For the optional items, the user can just press the Enter key to accept the default values.

Option name	Mandatory (M) or optional (O)	Description	Default value
New Load File	M	The name of the new GWC load file. The user must specify a name. Refer to procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 69.	
GWC List	M	The GWCs to be upgraded. By default, all GWC nodes managed by the CS 2000 Manager and SAM21 Manager are selected.	All
Load Directory	O	The GWC load directory configured in CS 2000 SAM21 Manage. The default value is '/swd/gwc'. If CS 2000 Core and Billing Manager (CBM) was used, the user must change the load directory to '/gwc'.	current configured load path
New Load Name	O	The target load name of the given GWC load file. If the file name does not contain the GWC load name, the user must specify a valid GWC load name here. The new load name is used to query the patch list from NPM. By default, the new load file name should be LOAD_NAME.imag, for example, gn070ch.imag, gn070ch.	new load file name (excluding '.imag')
Old Load Name	O	The load upgraded from. The default value is ' ' (null). If the user ignores this option (the default), the upgrade manager server bypasses old load checking and all selected GWC nodes are upgraded automatically.	old load file name (excluding '.imag')

Option name	Mandatory (M) or optional (O)	Description	Default value
Upgrade Mode	O	Defines whether GWCs are upgraded singly or together. Three modes are available: **single** - All GWC nodes are upgraded one by one, ordered by GWC profile type and GWC ID. **bulk** - All GWC nodes within the same service group (for example, TRUNK, LINE) are upgraded at the same time. If patching is needed, the first selected 'seed' GWC node which is used to create the soak image uses single mode, and the other nodes that do not need patching use bulk mode. **mix** - In the same GWC profile group (for example, Trunk GWCs, Line GWCs), one GWC node is upgraded first. This enables the user to verify a specific type of GWC. After the first node is upgraded successfully, all the other GWC nodes within the same profile group are upgraded together.	bulk
Pause Point	O	Specifies the points at which the upgrade process pauses to allow the user to make manual checks. Seven options are available: **0** - No pause points; if 0 is selected, all other pause points are ignored. **1** - Pause before locking the first unit of the 'seed' GWC node. **2** - Pause after patches are applied to the 'seed' node. **3** - Pause before warm swact of the 'seed' node. **4** - Pause after warm swact of the 'seed' node. **5** - Pause after the 'seed' node is upgraded. **6** - Pause before warm swact of 'non-seed' nodes. Pause points 1 to 5 apply only to the 'seed' GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.	0
Logging Level	O	Defines the default logging level of the GWC Upgrade Tool.	MAJ
Max Time	O	Defines the time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends. The default value **0** disables the time limit check.	0 (no time limit)

Option name	Mandatory (M) or optional (O)	Description	Default value
Alarm Level	O	Defines the alarm level of the in-service GWC unit that the GWC Upgrade Tool reports to the user. Values are: **MAJ** - major **CRT** - critical	MAJ
Alarm Number	O	Defines the acceptable alarm count, that is, the number of in-service GWC alarms of the specified alarm level at which the GWC Upgrade Tool reports to the user (see section Alarm checking on page 28 for details).	2

Alarm checking

During the upgrade only the in-service GWC unit is checked for alarms, and only the critical and major alarms are checked. When the actual GWC alarms reach the defined alarm state, the upgrade pauses and the system displays a message to the user.

For example, if the alarm checking is set to the default values ‘MAJ 2’, the following table shows how the GWC Upgrade Tool behaves when different numbers of in-service GWC alarms occur:

In-service GWC alarms	Upgrade pauses?
CRT 0, MAJ 1	N
CRT 0, MAJ 2	N
CRT 0, MAJ 3	Y
CRT 1, MAJ 0	Y
CRT 1, MAJ 1	Y
CRT 2, MAJ 0	Y
CRT 2, MAJ 1	Y
CRT 2, MAJ 2	Y

For a further example, if the alarm checking is set to the values ‘CRT 2’, the following table shows how the tool behaves when different numbers of in-service GWC alarms occur:

In-service GWC alarms	Upgrade pauses?
CRT 0, MAJ 1	N
CRT 0, MAJ 2	N
CRT 0, MAJ 3	N
CRT 1, MAJ 0	N
CRT 1, MAJ 1	N
CRT1, MAJ 2	N
CRT 2, MAJ 0	N
CRT 2, MAJ 1	N
CRT 2, MAJ 2	N
CRT 3, MAJ 0	Y

Upgrade procedure

At the CS 2000 Management Tool interface

1 **Check prerequisites**
Check the prerequisites as described in section Prerequisites and guidelines on page 23. Return to this procedure and carry out the additional prerequisite actions in steps 2, 3, and 5.

2 Ensure that you have a valid user ID and password to access the GWC Upgrade Tool.

a Telnet or SSH to the Sun server. Type:

```
> telnet <server>
```
or
```
> ssh -1 <user_ID> <server>
```
where <server> is the IP address or host name of the Sun server where CS 2000 SESM server resides.

and press the Enter key.

b When prompted, type your user ID and password, and press the Enter key.

3 Ensure that the operator belongs to one of the following groups authorized to launch the GWC Upgrade Tool: mgcmtc, mgcadm, emsmtc or emsadm. If necessary, refer to procedure "Setting up local user accounts on an SSPFS-based server" in *ATM/IP Solution-level Security and Administration*, NN10402-600. Type:

```
> id -a
```

and press the Enter key.

System response:

```
$ id -a
uid=104(ptm)  gid=105(succssn)
groups=105(succssn),1001(trkadm),1006(lnadm),
1011(mgcadm),1016(mgadm),1021(emsadm)
$
```

Group names

Note 1: CS 2000 SAM21 Manager must be installed in the same server as the GWC Upgrade Tool. CORBA, SESMService, NPM, and SAM21 Manager must be running in this server, otherwise the GWC Upgrade Tool cannot be launched.

Note 2: If NPM server is configured within the same server, it must be configured and running correctly. If NPM server is running with the Integrated EMS server, the PSE package within the same server must be configured and running correctly (and NPM may not appear in the system response below).

4 Refer to the following table to determine your next action.

If you are	Do
logged in as root	go to step 5
not logged in as root	change to the root user: type **su - root** , press the Enter key and continue at step 5

5 Check the status of the SAM21 element server and CORBA server to ensure they are running properly. Type:

```
> servquery -status all
```

and press the Enter key.

System response:

```
$ servquery -status all
APP NAME                STATUS
========                ======
DATABASE                RUNNING
CINOTIFIER              RUNNING
BACKUP_MANAGER          Group Started. Current status unavailable
BOOTP                   RUNNING
WEBSERVER               RUNNING
CORBA                   RUNNING
OMPUSH                  RUNNING
SESMService             RUNNING
WEBSERVICES             RUNNING
DDMSPROXY               RUNNING
ORA_AUTO_BACKUP         RUNNING
DELEGATE                RUNNING
ORA_ARCHIVE_ROTATOR     RUNNING
NPM                     RUNNING
PROP_SRV                RUNNING
SAM21EM                 RUNNING
SNMP_POLLER             Group Started. Current status unavailable
QCA                     RUNNING
```

Server states

6 Launch GWC Upgrade Tool

Exit from root and start the GWC Upgrade Tool CLUI. Type:

```
> exit
> cd /opt/nortel/NTsesm/gwcuptool/bin
> ./gwcuptool.sh
```

and press the Enter key.

System response:

```
cd /opt/nortel/NTsesn/gwcuptool/bin
./gwcuptool.sh
Starting ....

Main Menu for GWC upgrade tool
1 -  Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Within the GWC Upgrade Tool, after typing a menu option or other input value, press the Enter key. Details of the Main Menu options are as follows:

1 - Display all GWC nodes
This option is to query the name and card type for all GWC nodes.

Example system response:

```
Enter selection (1-4,x): 1

------------------------------------------------------------
GWC-7   TRUNKNA
GWC-0   SMALL_LINENA
GWC-2   SMALL_LINENA
GWC-3   LARGE_LINENA
GWC-4   SMALL_LINENA
GWC-5   SMALL_LINENA
GWC-6   SMALL_LINENA
------------------------------------------------------------
Total: 7
```

2 - Configure upgrade-related options
This option is to configure upgrade options manually. The CLUI prompts the user to input the necessary information step by step. These configuration options are then effective throughout the whole upgrade process.

3 - List current configuration values
This option lists all the configuration options currently applied.

4 - Enter Upgrade Menu
This option is to enter the upgrade submenu.

x - Stop upgrade tool and exit CLUI
This option stops the GWC Upgrade Tool and exits the CLUI.

7 Configure upgrade options

From the Main Menu, enter:

> 2

System response:

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration
[Step 1 - LOAD FILE NAME]
Enter the new load file name (Example: gn070bv.imag):
```

8 Enter the new GWC load file name. Ensure that the configured load file name exists in the load server (CS 2000 Core Manager or CBM).

Load name format:

nnnnnnn.nnnn

Example file name entry:

gn080bv.imag

System response:

```
Enter the new load file name (Example: gn070bv.imag): gn080bf.imag

[Step 2 - GWC LIST]
GWC list
Separate GWC nameS with commaS, for example: GWC-1,GWC-2,GWC-3,GWC-5.

Enter the GWC list (Default: all):
```

9 Enter the GWC nodes to be upgraded. To select all available GWCs, just press the Enter key. To select specific GWCs, enter the names of those required (with no spaces between the names).

Note: If you select all available GWCs, the GWC Upgrade Tool automatically upgrades the card types in the correct order (see GWC card type upgrade order on page 14).

Example list entry:

GWC-1,GWC-2,GWC-3,GWC-5

The system displays the current input configuration values.

Example system response:

```
Enter the GWC list (Default: all): GWC-2,GWC-4

[Step 3 - INPUT VALUES]
New Load File Name    : gn080bf.imag
GWC List              : GWC-2,GWC-4
Default values
Load Directory        : /swd/gwc/
New Load Name         : ""(ignored)
Old Load Name         : ""(ignored)
Upgrade Mode          : bulk
Pause Point           : 0 (none)
Logging Level         : MAJ
Max Time              : 0 (no limitation)
Alarm Level           : MAJ
Alarm Number          : 2

Do you want to use these configuration values? [Y|N] (Default: N):
```

10 Review the values displayed in the system response and refer to the following table to determine your next action.

If you want to	Do
use the values	enter **Y** and go to step 26
change the values	enter **N** and continue at step 12 ***Note:*** In the downgrade procedure, you must enter **N** to reject the default values, otherwise you cannot continue with step 12 and the rest of the downgrade steps.

11 *System response (after entering **N**):*

```
Do you want to use these configuration values? [Y|N] (Default: N): n

Do not use default values
[Step 4 - LOAD DIRECTORY]
Default load directory formats are different for SDM and CBM.
If SDM is used, it should be "/swd/gwc".
If CBM is used, it should be "/gwc".
Enter the load directory.  (Default: "/swd/gwc"):
```

12 Enter the load directory for CS 2000 Core Manager or CBM. The load directory formats are different, as listed below.

Note: The load directory must be as same as the “Load Info --> Path” value.

If you want to configure for	Do
CS 2000 Core Manager	enter **/swd/gwc**
CBM	enter **/gwc**

13 *System response (after pressing Enter):*

```
Enter the load directory. (Default: "/swd/gwc"): /swd/gwc

[Step 5 - NEW LOAD NAME]
Enter the new load name (Default: ""):
```

14 Enter the name of the new GWC load file. The load file name is used to query the patch list from NPM. If the file name does not contain the GWC load name, you must specify a valid GWC load name here, otherwise the GWC Upgrade Tool cannot retrieve the available patch list.

System response (after pressing Enter):

```
Enter the new load name (Default: ""):

[Step 6 - OLD LOAD NAME]
Enter the old load name (Default: ""):
```

15 Optionally, enter the name of the old GWC load file, that is, the file from which the load was upgraded. This is not normally needed; if you ignore this option, the upgrade manager server bypasses old load checking.

If you want to	Do
carry out a restricted upgrade, involving only GWCs running with a special load	enter the old GWC load file name
ignore this option ***Note:*** This is the recommended action.	press the Enter key

16 *System response (after pressing Enter):*

```
Enter the old load name (Default: ""):

[Step 7 - UPGRADE MODE]
Values:
1 - single
2 - bulk
3 - mix
h - help

Enter the upgrade mode (1-3,h), (Default: 2):
```

17 Enter the upgrade mode (see section Configurable options on page 26.

If you want to	Do
upgrade all configured GWC nodes one at a time (*single*)	enter **1**
upgrade all configured GWC nodes in the same service group simultaneously (*bulk*)	enter **2**
upgrade all configured GWC nodes in the same profile group simultaneously (*mix*)	enter **3**
accept the default (*bulk*)	press the Enter key

18 *System response (after pressing Enter):*

```
Enter the upgrade mode (1-3,h), (Default: 2):

[Step 8 - PAUSE POINTS]
Values:
0- no pause points

(1) For the first GWC node within the same GWC group.
1 - before locking first upgrade unit of "seed" node
2 - after patch applied to "seed" unit
3 - before warm-swact
4 - after warm-swact
5 - after "seed" node upgraded

(2) For bulk upgrade of GWC nodes with the same GWC service type.
6 - before warm-swact

Separate numbers with comma, for example: 1,3,4
Enter the pause points (Default: 0):
```

19 Enter the pause points for the upgrade (see section Configurable options on page 26). Pause points allow you to carry out manual checks at selected intervals during the upgrade process. Pause points 1 to 5 (see above screen) apply only to the patched 'seed' GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.

To accept the default value (0), just press the Enter key.

Example pause point entry:

```
Enter the pause points (Default: 0): 1,3
```

These entries allow two pause points:
before the first upgrade unit of the "seed" pair is locked ***(1)***
and before a warm SwAct ***(3)****.*

System response (after pressing Enter):

```
Enter the pause points (Default: 0):

[Step 9 - LOGGING LEVEL]
Values:
1 - Verbose
2 - Minor
3 - Major
4 - Critical

Enter the logging level (1-4),(Default: 3):
```

20 Enter the required logging level: VRB, MNR, MAJ or CRT (default: MAJ). Upgrade logs are stored in a file in upgrade.log under /opt/nortel/sam21em/logs/. Use the logs for troubleshooting.

To accept the default value (MAJ), just press the Enter key.

System response (after pressing Enter):

```
Enter the logging level (1-4),(Default: 3):

[Step 10 - TIME LIMIT]
Note: 0 means no time limit

Enter the time limit in minutes (Default: 0):
```

21 Enter a time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends.

The default value (0) disables the time limit check.To accept the default value, just press the Enter key.

In the Prepare step (see step 26), this value is compared with the estimated time for the upgrade. If the upgrade cannot be completed within the given time limit, the Prepare step fails.

System response (after pressing Enter):

```
Enter the time limit in minutes (Default: 0):

[Step 11 - ALARM LEVEL]
Values:
1 - Critical
2 - Major

Enter the alarm level (Default: 2):
```

22 Enter the required alarm level: CRT or MAJ. For details, refer to section Alarm checking on page 28.

To accept the default value (MAJ), just press the Enter key.

System response (after pressing Enter):

```
Enter the alarm level (Default: 2):

[Step 12 - ALARM NUMBER]

Enter the maximum allowed alarm number, (Default: 2)
```

23 Enter the maximum number of alarms allowed during the upgrade. For details, refer to section Alarm checking on page 28. If the current alarm state has a higher priority than the alarm number defined in this entry, the upgrade process pauses and the system notifies the user.

To accept the default value (2), just press the Enter key.

The entries in the example allow a maximum of two Major alarms during the upgrade process. In this case, if three Major alarms occur during the upgrade, the GWC Upgrade Tool pauses. If one Major alarm occurs, the tool ignores it and continues the upgrade process. If one Critical alarm occurs, the tool also pauses, because Critical alarms have a higher priority than Major alarms.

System response (after pressing Enter):

```
Enter the maximum allowed alarm number, (Default: 2)

Configuration values:
New Load File Name    : gn080bf.imag
GWC List              : GWC-2,GWC-4
Load Directory        : /swd/gwc
New Load Name         :
Old Load Name         :
Upgrade Mode          : bulk
Pause Point           : 0
Logging Level         : MAJ
Max Time              : 0
Alarm Level           : MAJ
Alarm Number          : 2

Is this information correct? [Y|N] (Default: N):
```

24 Check the upgrade configuration options. Review the values displayed in the system response (see above screen) and decide whether or not to proceed with the upgrade.

If	Do
you want to confirm the upgrade configuration options	enter **Y**. Note the following system response, and go to step 26
you do not want to confirm the upgrade configuration options	enter **N** , then return to step 7 to re-enter the options, or go to step 36 to exit the GWC Upgrade Tool

25 *System response (after entering **Y**):*

```
Is this information correct? [Y|N] (Default: N): y

Current configuration values:
 GWC load file: gn080bf.imag
 New load name: GN080BF
Load directory: /swd/gwc
  Working mode: bulk
Selected nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

Note: After confirming the configuration, you can display the current configuration settings at any time by selecting option 3 from the Main Menu.

Example system response:

```
Enter selection (1-4,x): 3

Current configuration values:
 GWC load file: gn080bf.imag
 New load name: GN080BF
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

26 **Prepare for upgrade**

On completion of the configuration steps, you must select the Upgrade Menu to carry out the actual upgrade. From the Main Menu, enter:

> 4

System response:

```
Enter selection (1-4,x): 4

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

27 In the Upgrade Menu, select the Prepare option. Enter:

> 1

Example system response:

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

[1 Prepare step]

The following patches are available in NPM.
  1, NBF00G08
  2, NBF01G08
  3, NBF02G08
  4, NBF03G08
  5, NBF04G08
  6, NBF05G08
  7, NBF06G08
  8, NBF07G08
  9, NBF08G08
  10, NBF09G08
  11, NBF11G08
  12, NBF12G08
  13, NBF13G08
  14, NBF14G08
  15, NBF15G08
  16, NBF17G08
Please disable the NPM automated processes.
```

28 Check that the load is available in CS 2000 Core Manager or CBM.

If the load	Do
is not available, the system displays the following message: `GWC load file doesn't exist. Please check and try later.` (see GWC load not available on page 55)	return to step 8
is available	continue at step 29

29 Disable the NPM automated processes.

a Log in to the NPM GUI:
- Select "System" from the tool bar.
- Select "Plans..." from the menu.
- Click on the "Plan List" tab.
- If any of the plans in the list have "Enabled" checked, they must be disabled. For each plan that is enabled, highlight the plan in the menu and click on the "Disable" button at the bottom.

OR

Log in to the NPM CLUI:
- Execute the command: getplan
- If any of the plans in the list have "Enabled" set to "Y", they must be disabled. For each plan that is enabled, execute the following to disable it:
enableplan <planname> OFF

b Keep a record of the plans that were disabled. These plans must be re-enabled at the end of the upgrade process.

30 Display and confirm the patch list.

Note: You must be assigned to user group "emsadm" to perform patching activities using the NPM.

a If patches were delivered on CD, insert the CD that contains the patches into the CD drive of the Sun server where NPM resides.

b Telnet to the Sun server where the NPM resides.

c When prompted, type your user ID and password, and press the Enter key.

d Change to the root user. Type **su - root** and press the Enter key.

e When prompted, type the root password and press the Enter key.

f If patches were delivered electronically, go to step l; otherwise continue at step g.

g Patches on CD:
Make a temporary directory for the patchlist file.
Type **mkdir /data/npm/tmp** and press the Enter key.

h Change the permissions on the temporary directory.
Type **chmod 777 /data/npm/tmp** and press the Enter key.

i In the temporary directory, create the .patchlist file for all the patches on the CD. Type **find /cdrom -name '*.patch' > /data/npm/tmp/current.patchlist** and press the Enter key.

j Access the directory you just created.
Type **cd /data/npm/tmp** and press the Enter key.

k Go to step v.

l Patches delivered electronically:
Make a directory for the patch files you want to install.
Type **mkdir /data/npm/patch_upgrade** and press the Enter key.

m Change the permissions on the newly created directory.
Type **chmod 777 /data/npm/patch_upgrade** and press the Enter key.

n Access the newly created directory.
Type **cd /data/npm/patch_upgrade** and press the Enter key.

o FTP to the ESD server. Type **ftp** <ESD_server> and press the Enter key.

p When prompted, type your user ID and password for the ESD server, and press the Enter key.

q Set the transfer mode to binary. Type **ftp> bin** and press the Enter key.

r Transfer all the patches from the ESD server to the NPM.
Type **ftp> mget *.patch** and press the Enter key.

s Exit FTP. Type **ftp> quit** and press the Enter key.

t Verify that the patches are in the temporary directory on the Sun server. Type **ls** and press the Enter key.

u Change the permissions for the patch files in the directory. Type **chmod 777 *** and press the Enter key.

v Retrieve the patch files:
Verify that the NPM server application is running.
Type **servquery -status -group NPM** and press the Enter key.

Note: The NPM can be started by typing **servstart NPM**.

w Access the NPM command line user interface (CLUI).
Type **npm** and press the Enter key.

x When prompted, type your user ID and password, and press the Enter key.

y Retrieve the patch files for the NPM to process as follows:
- For patches from CD-ROM, type **npm> getpatch current.patchlist** and press the Enter key.
- For patches from ESD, type **npm> getpatch** <patch_filename> and press the Enter key.
where <patch_filename> is the name of the file that contains names of the patch files to retrieve (name must end with ".patchlist"), or an actual patch file.

z Exit the NPM CLUI. Type **npm> quit** and press the Enter key.

aa Change directory. Type **cd** and press the Enter key.

Note: You must change directory from the cdrom directory for the next command (eject cdrom) to execute successfully.

ab Eject the CD from the drive. Type **eject cdrom** and press the Enter key.

Example system response:

```
--{ Group-1 }-----------------------------------------------------
  GWC-2 SMALL_LINENA

--{ Group-2 }-----------------------------------------------------
  GWC-4 SMALL_LINENA
------------------------------------------------------------------------
Estimated Time:  1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

The system displays the GWC upgrade plan and estimated upgrade time, then returns to the Upgrade Menu.

31 Perform pre-check

In the Upgrade Menu, select the Pre-check option. Enter:

> 2

Example system response:

```
Enter selection (1-5,x): 2

[2 Pre-check step]

--{ Group-1 }-----------------------------------------------------
  GWC-2 SMALL_LINENA ... passed

--{ Group-2 }-----------------------------------------------------
  GWC-4 SMALL_LINENA ... passed
------------------------------------------------------------------------
Total:  1 hour 5 minutes 30 seconds

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

32 Check the pre-check conditions. Review the information in the system response (see above screen) as follows:

a Check that the CS 2000 GWC Manager, SAM21 Manager, and NPM servers are running.

b Check that neither GWC card has a hardware alarm.

c Verify that one GWC card is in service, and the other card is hot-standby.

If	Do
any of the pre-check conditions is not met (see Pre-check failure on page 55)	resolve the error conditions (go to step 4 to activate the servers, clear any hardware alarms, correct the status of the GWC cards), then continue the upgrade process at step 33
all the pre-check conditions are met (the screen displays "`passed`")	continue the upgrade process at step 33

33 **Upgrade GWC nodes**

In the Upgrade Menu, select the Upgrade option. Enter:

```
> 3
```

Internal procedures

At the start of the upgrade, the GWC Upgrade Tool performs the pre-check again. During the upgrade, the system displays a continuous log of the upgrade status (the log freezing may indicate a problem with one of the internal upgrade procedures). You can also use the query option (see Query upgrade status on page 50) to display the upgrade status. If any unexpected problems occur, the system normally prompts you for a response or confirmation before continuing.

If pause points were enabled during configuration (see step 19), the tool pauses at the specified points and waits for you to carry out the required manual checks. When you have finished, enter **Continue** to continue the upgrade.

During the upgrade, the GWC firmware flash is enabled automatically.

There are two different internal upgrade procedures:

- For the 'seed' GWC node there are 16 steps. The 'seed' node is based on the upgrade order of the GWC card types, and GWC node ID. The GWC Upgrade Tool automatically selects

the ‘seed’ node from the GWC list entered by the user (see step 9).

- For all other (‘non-seed’) nodes there are 11 steps. The tool automatically upgrades the other nodes when the ‘seed’ is upgraded successfully.

Example system response - ‘seed’ node:

```
Enter selection (1-5,x): 3

[3 Upgrade step]

--{ Group-1 }------------------------------------------------------
  GWC-2 SMALL_LINENA

--{ Group-2 }------------------------------------------------------
  GWC-4 SMALL_LINENA
------------------------------------------------------------------
Estimated Time:  1 hour 5 minutes 30 seconds

--{ Group-1 }------------------------------------------------------
  GWC-2 SMALL_LINENA ... passed

--{ Group-2 }------------------------------------------------------
  GWC-4 SMALL_LINENA ... passed
------------------------------------------------------------------
Total:  1 hour 5 minutes 30 seconds

Group-1 started
GWC-2: Upgrade task is started.
GWC-2 [1/16]  Busy the hot-standby first unit.(GWC-2-UNIT-1)
GWC-2 [2/16]  Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16]  Change the load of locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16]  Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16]  Waiting for the first unit to be hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16]  Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16]  Patches are applied with the upgraded first unit (GWC-2-UNIT-1)
GWC-2 [9/16]  Waiting for the patched unit to be hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16] Patched unit is hot-standby, load imaging is started(GWC-2-UNIT-1)
GWC-2 [11/16] GWC load imaging is finished. Perform the warm-swact(GWC-2-UNIT-0)
GWC-2 [12/16]  Warm-swact is finished, busy the second unit. (GWC-2-UNIT-0)
GWC-2 [13/16]  Locking the second unit. (GWC-2-UNIT-0)
GWC-2 [14/16]  Second unit is locked. (GWC-2-UNIT-0)
GWC-2 [15/16]  Change load of the locked second unit. (GWC-2-UNIT-0)
GWC-2 [16/16]  Second unit is booted up with the soaked load. (GWC-2-UNIT-0)
GWC-2 Upgrade finished successfully.
Group-1 finished
  Elapsed Time: 16 minutes 25 seconds
Remaining Time: 24 minutes 15 seconds
```

Upgrade steps for the ‘seed’ GWC node

This section assumes that GWC-2 is the ‘seed’ node, GWC-2 UNIT-0 is in service, GWC-2 UNIT-1 is hot-standby, the new load file name is gn080as.imag, and the load version is GN080AS.

The GWC Upgrade Tool automatically performs the following actions:

1. Busies the inactive unit GWC-2 UNIT-1 in the GWC EM.
2. Locks the inactive unit GWC-2 UNIT-1 in the SAM21 EM.
3. Provisions GWC-2 UNIT-1 with the new load gn080as.imag in the SAM21 EM.
4. Unlocks GWC-2 UNIT-1 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-2 UNIT-1 to become hot-standby.
6. Busies the upgraded GWC-2 UNIT-1 in the GWC EM.
7. Carries out a device audit against GWC-2 UNIT-1 in NPM.
8. Applies all available patches to GWC-2 UNIT-1 in NPM.
9. Returns To Service the patched GWC-2 UNIT-1 in the GWC EM.
10. Waits for GWC-2 UNIT-1 to become hot-standby.
11. Saves the soaked GWC image into CS 2000 Core Manager or CBM in the GWC EM.

    Note: The gn080as.imag is now a soaked load which contains all applicable patches for the GN080AS load.

12. Warm swacts the GWC-2 nodes: GWC-2 UNIT-1 provides service, and GWC-2 UNIT-0 is hot-standby.
13. Locks the inactive second unit GWC-2 UNIT-0 in the SAM21 EM.
14. Provisions GWC-2 UNIT-0 with the new soaked load gn080as.imag in the SAM21 EM.
15. Unlocks GWC-2 UNIT-0 in the SAM21 EM.
16. Waits for the inactive/upgraded GWC-2 UNIT-0 to become hot-standby.

Example system response - 'non-seed' nodes:

```
Group-2 started
GWC-4: Upgrade task is started.
GWC-4 [1/11]  Busy the hot-standby first unit. (GWC-4-UNIT-0)
GWC-4 [2/11]  Lock the inactive first unit. (GWC-4-UNIT-0)
GWC-4 [3/11]  Change the load of locked first unit. (GWC-4-UNIT-0)
GWC-4 [4/11]  Unlock the first unit. (GWC-4-UNIT-0)
GWC-4 [5/11]  Waiting for the first unit to be hot-standby. (GWC-4-UNIT-0)
GWC-4 [6/11]  First unit is hot-standby. Perform the warm-swact. (GWC-4-UNIT-1)
GWC-4 [7/11]  Warm-swact is finished, busy the second unit. (GWC-4-UNIT-1)
GWC-4 [8/11]  Locking the second unit. (GWC-4-UNIT-1)
GWC-4 [9/11]  Second unit is locked. (GWC-4-UNIT-1)
GWC-4 [10/11]  Change load of the locked second unit. (GWC-4-UNIT-1)
GWC-4 [11/11]  Second unit is booted up with the soaked load. (GWC-4-UNIT-1)
GWC-4 Upgrade finished successfully.
Group-2 finished
 Elapsed Time: 26 minutes 2 seconds
```

Upgrade steps for the 'non-seed' GWC nodes

This section assumes that GWC-4 is a 'non-seed' node, GWC-4 UNIT-1 is in service, GWC-4 UNIT-0 is hot-standby, the new load file name is gn080as.imag, and it is a soaked load which contains all applicable patches for the GN080AS load.

The GWC Upgrade Tool automatically performs the following actions:

1. Busies the inactive unit GWC-4 UNIT-0 in the GWC EM.
2. Locks the inactive unit GWC-4 UNIT-0 in the SAM21 EM.
3. Provisions GWC-4 UNIT-0 with the new soaked load gn080as.imag in the SAM21 EM.
4. Unlocks GWC-4 UNIT-0 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-4 UNIT-0 to become hot-standby.
6. Warm swacts the GWC-4 nodes: GWC-4 UNIT-0 provides service, and GWC-4 UNIT-1 is hot-standby.
7. Busies the hot-standby GWC-4 UNIT-1 in the GWC EM.
8. Locks the inactive second unit GWC-4 UNIT-1 in the SAM21 EM.
9. Provisions GWC-4 UNIT-1 with the new soaked load gn080as.imag in the SAM21 EM.
10. Unlocks GWC-4 UNIT-1 in the SAM21 EM.
11. Waits for the inactive/upgraded GWC-4 UNIT-1 to become hot-standby.

Pause conditions

During upgrade, the system may pause, because manual actions are needed, or an operation has failed. The table below shows the various pause conditions and the user action required:

If	Do
the current upgrade state is a pause point that you configured (see step 19, and Pause point on page 57)	carry out the required manual check, then enter **Continue** to continue the upgrade
NPM requires manual actions to be taken during the patching step (see Patch problem on page 58)	launch the NPM GUI or CLUI to perform the required actions, then return to the GWC Upgrade Tool and enter **Continue** to continue the upgrade
the GWC alarms (in the in-service unit) exceed the configured alarm level (see steps 22 and 23, and Alarm level exceeded on page 59)	refer to section Alarm checking on page 28
an operation failed when the tool invoked the GWC EM, SAM21 EM or NPM functions (e.g. the GWC EM cannot save the GWC load image to CS 2000 Core Manager or CBM)	check and rectify the failed operation manually, then enter **Retry** to continue the upgrade
an operation timeout occurs (e.g. the upgraded inactive unit is not hot-standby; see Operation timeout on page 60)	carry out the timed-out operation manually, then enter **Retry** to continue the upgrade

Query upgrade status

While the upgrade is in progress, you can launch another telnet or SSH session to the server, and use the following command to query the overall status of the upgrade:

/opt/nortel/NTsesm/gwcuptool/bin/gwcuptool.sh -query

34 When the upgrade finishes, the system reports the final service status of the upgraded GWC nodes and returns to the Upgrade Menu.

System response:

```
--{ Group-1 }--------------------------------------------------------------------
               GWC Node: GWC-2
                Profile: SMALL_LINENA
                 Status:  Upgrade finished successfully.
.
.
.
--{ Group-2 }--------------------------------------------------------------------
               GWC Node: GWC-4
                Profile: SMALL_LINENA
                 Status:  Upgrade finished successfully.
.
.
.
States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

35 Perform post-check

In the Upgrade Menu, select the Post-check option. Enter:

> 5

Example system response:

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

[5 Post-check step]

--{ Group-1 }-------------------------------------------------------------------
              GWC Node: GWC-2
               Profile: SMALL_LINENA
                Status:  Upgrade finished successfully.
            Start time: Mon Dec 13 05:36:12 EST 2004
             Stop time: Mon Dec 13 05:52:36 EST 2004
          Elapsed time: 16 minutes 23 seconds
    GWC-2-UNIT-1: 47.142.128.51
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-2-UNIT-0: 47.142.128.50
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: hotStandby(1)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

--{ Group-2 }-------------------------------------------------------------------
              GWC Node: GWC-4...
```

The screen display repeats the service status of the upgraded GWC nodes. The post-check checks the status of all the upgraded nodes, to ensure that:

- there is no alarm for the in-service GWC unit
- one unit is in service, and the other unit is hot-standby

36 **Exit GWC Upgrade Tool**

When the post-check finishes, pressthe Enter key to return to the Upgrade Menu.

System response:

```
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

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

37 Exit the Upgrade Menu and return to the Main Menu. Enter:

> x

System response:

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

Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x):
```

38 Use the following table to determine your next step.

If	Do
you want to upgrade further GWC nodes	go back to step 7
all the required GWCs have been upgraded	continue at step 39

39

CAUTION

Do not exit the GWC Upgrade Tool before the upgrade finishes successfully. Do not press 'Ctrl+C' or close the TERM. If you do so and then start the GWC Upgrade Tool again, the system displays the message:

```
Warning!!! One Upgrade Manager is
running already. It is not recommended
to start a new server. Start a new one
to override it? (default N) Y/N):
```

Stop the GWC Upgrade Tool and exit the CLUI. Enter:

> x

Example system response:

```
Enter selection (1-4,x): x
GWC Upgrade Manager server stopped.
comp5iems-unit0(active):/export/home/ptm>
```

40 This procedure is complete.

Example screens

GWC load not available

If the GWC load is not available, the Prepare step fails. You must verify that the GWC load file is installed correctly, then return to the Configuration step to re-input the file name.

```
Main Menu for GWC upgrade tool
1 - Display all GWC nodes
2 - Configure upgrade-related options
3 - List current configuration values
4 - Enter Upgrade Menu

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration
[Step 1]
Enter new load file name(Example: gn070bv.imag): gn080be.imag
.
.
.
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 1
 GWC load file doesn't exist.
Available GWC loads in the given directory in SDM/CBM:
  - GwcConfig.sh
  - gn080bf.imag
  - gn080bf_jg.imag
  - gn080bg1.imag
```

Pre-check failure

There are several conditions which may cause the Pre-check step to fail, for example, servers not running, GWC cards with incorrect status. You must correct the problem, then repeat the Pre-check step.

```
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 2

--{ Group-1 }------------------------------------------------------------
  GWC-10        LARGE_LINENA ... failed
              GWC Node: GWC-10
               Profile: LARGE_LINENA
                Status:  Auto discovery in progress.
        Estimated time: 41 minutes 15 seconds
                Paused: Invalid GWC status, unable to perform the upgrade.
    GWC-10-UNIT-0: 47.142.128.158
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: locked(2)
     Operational state: disabled(2)
        Stand by state: coldStandby(2)
           Fault state: none(0)
           Alarm state: minor(3) , alarmOutstanding(4)
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-10-UNIT-1: 47.142.128.159
     States from GWCEM:
     Current load name: GN080BF
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: major(2) , alarmOutstanding(4)
            - Critical: 0
               - Major: 1
    1, Communication with a gateway is down. (MG10/00/5)
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
```

Pause point

Pause points occur during the upgrade process wherever you specified them in the Configuration step. You must carry out the required manual checks, then enter **Continue** to allow the upgrade process to continue.

```
[Step 8]
Pause points.
 1) For the first GWC node within the same GWC group.
    1. before lock the first upgrade unit of "seed" node.
    2. after patch applied to the "seed" unit.
    3. before warm-swact.
    4. after warm-swact.
    5. after "seed" node upgraded.
 2) For bulk upgrade GWC nodes with same GWC service type.
    6. before warm-swact.

    0. no pause point. If 0 applied, ignore all other pause points.
 Example: 1,3,4
Enter pause point (Default: 0):1,2,3,4,5

[Step 9]
Logging level selection
.
.
.
Group-1 started
Upgrade task started
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-1)
GWC-10 [2/16]  Lock the inactive first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: before lock the first upgrade unit.
Please select from following:
Continue

Answer: continue
GWC-10 [3/16]  Change the load of locked first unit. (GWC-10-UNIT-1)
GWC-10 [4/16]  Unlock the first unit. (GWC-10-UNIT-1)
GWC-10 [5/16]  Waiting for the first unit to be hot-standby. (GWC-10-UNIT-1)
GWC-10 [6/16]  Upgraded first unit is hot-standby. (GWC-10-UNIT-1)
GWC-10 [7/16]  Apply patch to the upgraded first unit. (GWC-10-UNIT-1)
Apply request was attempted by the NPM server.
GWC-10 [8/16]  Patches are applied with the upgraded first unit. (GWC-10-UNIT-1)

Message received from the server:

GWC-10 CHECK-POINT: patches are applied for the "seed" unit.
Please select from following:
Continue
Answer: Continue
GWC-10 [9/16]  Waiting for the patched unit to be hot-standby (GWC-10-UNIT-1)
.
```

Patch problem

To ignore the error and allow the upgrade process to continue, you can simply enter **Continue** . If some manual action is needed (for example, launching the NPM CLUI/GUI), carry out the required action, then enter **Continue**. To invoke the NPM to attempt to apply the patch again, enter **Retry**. To abort the upgrade for the current GWC node, enter **Abort**.

```
Group-1 started
GWC-2: Upgrade task is started.
GWC-2 [1/16]  Busy the hot-standby first unit. (GWC-2-UNIT-1)
GWC-2 [2/16]  Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16]  Change the load of locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16]  Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16]  Waiting for the first unit to be hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16]  Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Patch NBF01G08 requires special attention:
  Ftp Error command
Patch NBF02G08 requires special attention:
  ERROR: Patch NBF01G08 needs to be applied in GWC-2-UNIT-1 before NBF02G08 can be
applied.
Patch NBF03G08 requires special attention:
  ERROR: Patch NBF01G08 needs to be applied in GWC-2-UNIT-1 before NBF03G08 can be
applied.
.
.
.
Message received from the server:

GWC-2 Warning: NPM can't apply all patches to GWC unit. GWC-2-UNIT-1
Please select from following:
Continue Retry Abort

Answer: retry
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Apply request was attempted by the NPM server.
GWC-2 [8/16]  Patches are applied with the upgraded first unit. (GWC-2-UNIT-1)
GWC-2 [9/16]  Waiting for the patched unit to be hot-standby (GWC-2-UNIT-1)
GWC-2 [10/16]  Patched unit is hot-standby, load imaging is started.
(GWC-2-UNIT-1)
.
.
.
```

Alarm level exceeded

If the actual GWC alarms reach the alarm level defined in the Configuration step, the upgrade pauses. To ignore the alarms and allow the upgrade process to continue, you can simply enter **Continue**. Otherwise you must enter **Abort** to stop the upgrade, and correct the problem before continuing.

```
Group-1 started
Upgrade task started
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-1)
    GWC-10-UNIT-0: 47.142.128.158
     States from GWCEM:
     Current load name: GN080BE
  Administrative state: unlocked(1)
     Operational state: enabled(1)
        Stand by state: providingService(3)
           Fault state: none(0)
           Alarm state: major(2) , alarmOutstanding(4)
            - Critical: 0
               - Major: 1
    1, Communication with a gateway is down. (MG10/00/5)
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

Message received from the server:

GWC-10 In service unit has more alarms in GWCEM than configured. GWC-10-UNIT-0
Please select from following:
Continue Abort

Answer: Continue
GWC-10 Ignore the alarm states, and continue the upgrade task
```

Operation timeout

If an operation timeout occurs, the upgrade does not necessarily fail. You can use the CMT client and SAM21EM client to check the status of the GWC card. After performing the timed-out operation manually (for example, locking the GWC card), you can enter **Retry** to allow the upgrade process to continue.

```
Group-1 started
GWC-10: Upgrade task is started.
GWC-10 [1/16]  Busy the hot-standby first unit. (GWC-10-UNIT-0)
GWC-10 [2/16]  Lock the inactive first unit. (GWC-10-UNIT-0)

Message received from the server:

GWC-10 Timeout: SAM21EM can't lock the inactive GWC unit. GWC-10-UNIT-0
Please select from following:
Retry Abort

Answer: retry
GWC-10 [3/16]  Change the load of locked first unit. (GWC-10-UNIT-0)
.
.
.
```

Downgrade procedure

In SN08, the GWC Upgrade Tool (Phase 1) does not support an automated rollback procedure. However, as long as the upgraded GWC has not been provisioned with new data (for example, gateways, carriers, lines), the tool can be used to switch between the old and new loads, as described below.

At the CS 2000 Management Tool interface

1 Perform steps 1 to 10 of Upgrade procedure on page 29.

Note: At step 10 you must enter **N** to reject the default values, otherwise you cannot continue with step 12 and the rest of the downgrade procedure.

System response:

```
.
.
.
Do you want to use these values to configure (Default: N)? [Y|N]: n

Do not use default values
[Step 4]
Enter load directory. Default load directory formats are different for SDM and
CBM. If SDM is used, it should be "/swd/gwc". If CBM is used, it should be "/gwc".
(Default: "/swd/gwc"): /swd/gwc

[Step 5]
Enter new load name (Default: ""):
```

2 Enter the name of the old GWC load image file, that is, the original load that existed before the automatic upgrade started. The load name is used to query the patch list from NPM. If the load name does not contain the GWC load name, you must specify a valid GWC load name here, otherwise the GWC Upgrade Tool cannot retrieve the available patch list.

System response:

```
[Step 5]
Enter new load name (Default: ""): G1070CH

[Step 6]
Enter old load name: (Default: “”):
```

3 Enter the name of the new GWC load image file, that is, the load that was used in error during the automatic upgrade.

System response:

```
[Step 6]
Enter old load name (Default: ""): G1080BH

[Step 7]
Upgrade mode selection
 1 - single 2 - bulk 3 - mix
 h - help

Enter selection (1-3,h), (Default: 2):
```

4 Perform steps 15 to 41 of Upgrade procedure starting on page 35. The GWC Upgrade Tool reboots the GWC cards using the old load.

Re-provision the Ethernet Routing Switch 8600 port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Ethernet Routing Switch 8600.

Note: Make sure you use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to the Ethernet Routing Switch 8600 documentation and choose Getting Started.

At the CLI for the Ethernet Routing Switch 8600

1 Determine the slot and port on the router that connects to the device. Type:

> show ip arp info <ip_address>

and press the Enter key.

where **<ip_address>**
is the physical IP address of the GWC card

Example system response:

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                        Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

Note the slot and port number; you will need this information in the next step of this procedure.

Note: If the response indicates MLT instead of the slot and port, perform this operation from the mate unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.

2 Use the numbers recorded in step 1 on page 62 to set the slot and port to auto-negotiate. Type:

> config ethernet <slot>/<port> auto-negotiate enable

and press the Enter key.

System response:

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

The system configures the slot and port to auto-negotiate, and the prompt returns.

3 Verify the port configuration. Type:

> show ports info config <slot>/<port>

and press the Enter key.

System response:

```
prompt:cpu> show ports config info 1/2

================================================================================
                                    Port Config
================================================================================

PORT                AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE          NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX     true  false  half  100   full  100   fals  core  1   0
```

The system displays the slot and port configuration.

4 Commit the change. Type:

> save config

and press the Enter key.

5 Go to step 6 on page 31 to continue with the procedure "Upgrading the GWC using the GWC Upgrade Tool".

Overall upgrade process - manual

This section outlines the original manual process for upgrading selected Gateway Controllers (GWC) and applying patches.

Note 1: If you wish to use the new GWC Upgrade Tool, which upgrades selected GWCs and applies patches automatically, refer to procedure Overall GWC upgrade process - automated on page 19.

Note 2: Before you begin, make sure that you have researched and addressed all pre-upgrade items described in section Prepare to upgrade the gateway controller on page 13.

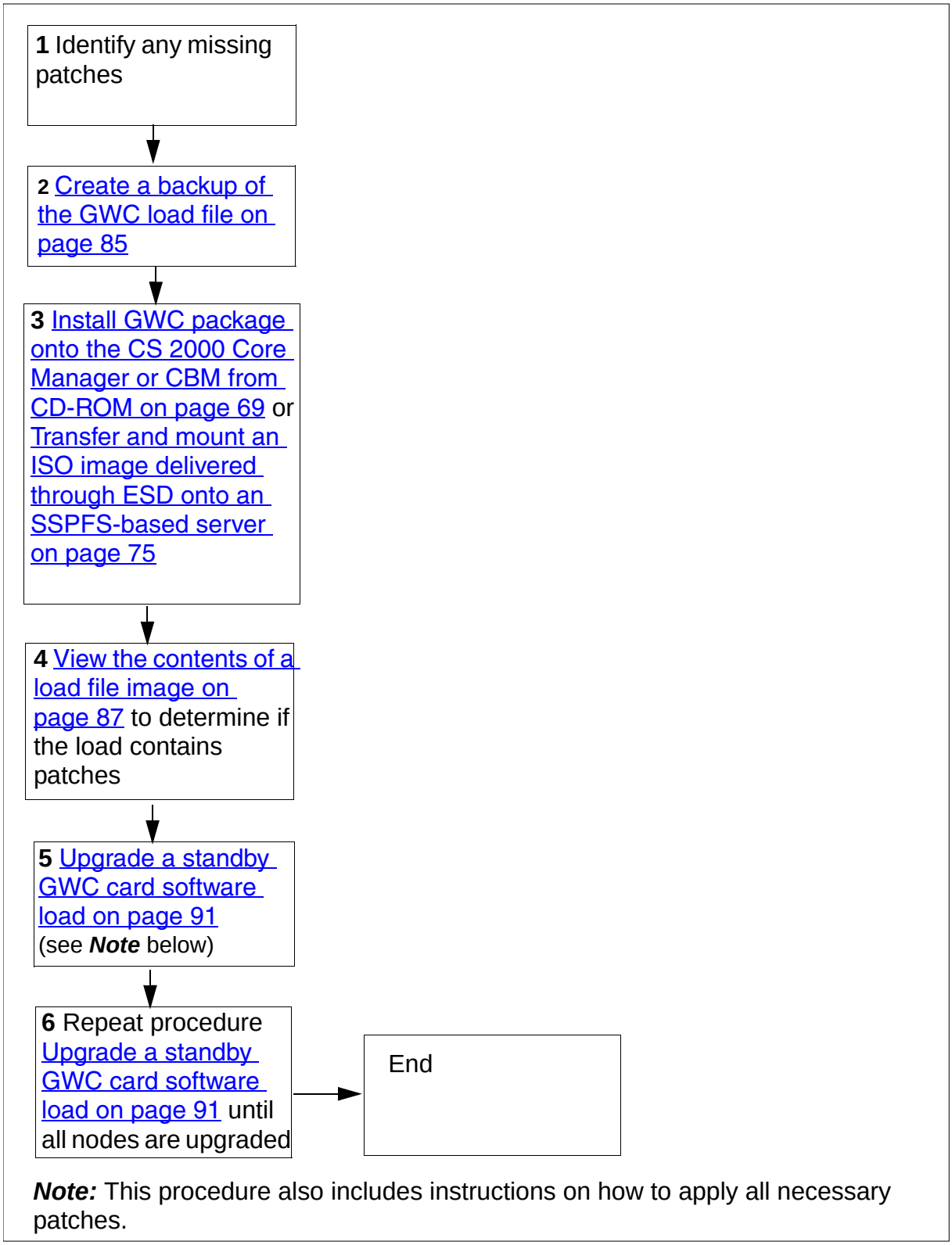
ATTENTION

For IP network solutions only (starting in SN07), the call agent identifier (ID) must be set for the CS 2000. Typically, this should be done prior to upgrading your GWC cards. For details, refer to section “CS 2000 call agent identifier” in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Summary flowchart

The following flowchart summarizes the overall GWC upgrade process. The numbers relate to the steps of the detailed procedure in section Overall GWC upgrade procedure on page 67 following the flowchart.

Summary of the overall GWC upgrade procedure



Note: This procedure also includes instructions on how to apply all necessary patches.

Overall GWC upgrade procedure

1 If necessary, complete the sub-steps (a) and (b) using one of the tools available at www.nortelnetworks.com. To obtain the tools:

- Under Support & Training, select Software Downloads.
- Select the Browse Product Support tab (this is usually the default choice).
- Follow the three steps displayed on the page:
  Step 1 - Product Families: select Succession or Succession Communication Server 2000.
  Step 2 - Product menu: select Communication Server 2000.
  Step 3 - Content menu: select Tools, then press 'Go'.
- For instructions on how to use each tool, refer to the Readme file that can be found under each corresponding link.

a Identify patches that have been released against your CD-ROM after it has been shipped - use the Pre Upgrade Patch Calculator tool. Download these patches (if any) to site and retrieve the patch files for the NPM to process using the NPM CLUI **getpatch** command.

b Perform site-specific audit to identify any missing patches - use the Patch Audit for Inform List tool.

2 If necessary, backup your existing software load using procedure Create a backup of the GWC load file on page 85.

3 If necessary, install the new load using one of the following methods:

- Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 69
- Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 75

4 See if any patches are contained within the load image by completing procedure View the contents of a load file image on page 87.

5 If a day or more has passed between completing step 1a and performing the upgrade, repeat step 1b, then continue the procedure.

6 Upgrade software on a seed GWC unit that is inactive using procedure Upgrade a standby GWC card software load on

page 91. The upgrade process includes the following main steps (for detailed instructions, refer to the procedure):

- Busy the standby card.
- Lock the standby card.
- Apply the new load name to the standby card.
- Unlock the card.
- If required, apply all necessary patches.
- Perform a warm switch of activity (SwAct).
- Upgrade the new standby (previously active) unit using the same procedure.

7 Repeat step 6 to upgrade each GWC node with the patched load until all units in each node are rebooted from the new image.

Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM

Purpose of this procedure

This procedure describes how to install GWC software loads onto the CS 2000 Core Manager or Core and Billing Manager (CBM) from CD-ROM. The software load is installed in the /swd/gwc directory on the CS 2000 Core Manager or CBM.

Note: For information on how to deliver and install GWC load using the Electronic Software Delivery (ESD) method, refer to procedure Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 75.

When to use this procedure

Use this procedure to install a Maintenance Non-Computing Load (MNCL) or a standard software release (NCL) GWC load.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Management Tools frame (Sun Microsystems t1400 or 240)

1 Insert the CD-ROM into the CD-ROM tray.

At the CS 2000 Management Tools terminal

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

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

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

3 Execute the installation script by typing

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

and pressing the Enter key.

Example response:

```
        Welcome to the Platform Installation Tool Version 3.3
 ================================================================
   RPM INSTALLATION/REMOVAL
  ============================
  1) Install RPM from CDROM        2) Install RPM from Disk
  3) Uninstall RPM                 4) Query all RPMs

  TAR INSTALLATION/REMOVAL
  ============================
  5) Install SC load from Tape     6) Install SC load from cdrom
  7) Install SC load from Disk     8) Remove a SC Load
  9) Install 3PC Load from Tape   10) Install 3PC Load from Disk

  OTHER
  ======
 L) Install SOS/MS/PMLOADS      D) Install SOS/MS/PMLOADS from disk
  C) Change Rotation Parameters  P) View Rotation Parameters
  V) Platform Version Installed  X) Exit

  Please choose one of the following: 1
```

4 Install the software by typing

> 1

and pressing the Enter key.

The system displays the contents of the .rpm package.

Example response:

```
           Verifying CDROM is mounted
 /cdrom/cdrom on /vol/dev/disk/c0t0d0/cdrom read
 only/mosuid/mapl-case/noglobal/rr/traildot/dev=16c0001
 on Sat Mar 27 16:34:13 2004
             CDROM is mounted.
             Listing file names in the rpm on the cd.
/swd/gwc/gwcConFig.sh
/swd/gwc/gn070be.imag

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

Note: If the system displays the following message: `There is no cd in the CDROM drive, please check drive`, ensure that the CD-ROM is inserted in the tray for this unit.

5 Confirm that you want to proceed with the installation by typing

`> Y`

and pressing the Enter key.

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

Example response:

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

Installing RPM package gn070be_plat-1.0-041304.moarch.rpm
Sun Microsystems Inc.  Sun 5.8   Generic Patch  December 2002
gn070be_plat-1.0-041304.noarch.rpm  100% 11MB 750.4KB   00:14
root@47.135.214.127's password: <enter root password>
```

6 Type the root password for the CS 2000 Core Manager or the CBM and press the Enter key.

The system installs the software on the CS 2000 Core Manager or CBM. If CBM is used, the .rpm package is then copied to the inactive CBM unit and another prompt for the root password is displayed. If this happens, type the root password again and press the Enter key.

After the load file is installed on the CS 2000 Core Manager or CBM, the transferred .rpm package is deleted from the CS 2000 Core Manager or CBM.

Example response:

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

Installing RPM package gn070be_plat-1.0--41304.moarch.rpm
Sun Microsystem Inc.  SunOs 5.8  Generic Patch December 2002
gn070be_plat-1.0-041304.noarch.rpm  100% 11MB 8.2MB/s   00:40
root@47.135.214.127's password: <enter root password>
Mate IP is 47.135.214.129
Sun Microsystem Inc.  SunOs 5.8  Generic Patch December 2002
root@47.135.214.129's password: <enter root password>


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

7 Exit the installation program by typing

 # x

and pressing the Enter key.

8 Use the following table to determine your next step.

If the GWC load is being installed on the	Do
CS 2000 Core Manager	go to step 9
CBM	go to step 15

At the CS 2000 Core Manager console or terminal window

9 Log in to the CS 2000 Core Manager as the root user.

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

10 Access the gwc directory by typing

 # cd /swd/gwc

and pressing the Enter key.

11 Execute the GwcConfig.sh script by typing

 # ./GwcConfig.sh

and pressing the Enter key.

Note: The script checks if the appropriate configuration data is present in the gwc directory. If the data is not present, the system prompts you to enter the hostname and the IP address of the SAM21 EM server.

12 If prompted, type the hostname of the SAM21 EM server and press the Enter key. Otherwise, continue with step 14.

13 If prompted, type the IP address of the SAM21 EM server and press the Enter key. Otherwise, continue with step 14.

14 Log out of the CS 2000 Core Manager by typing

 # exit

and pressing the Enter key.

At the CS 2000 Management Tools terminal

15 Eject the CD-ROM from the CD-ROM tray by typing

```
# eject cdrom
```

and pressing the Enter key.

16 Log out of the CS 2000 Management Tools server.

17 This procedure is complete.

Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server

Application

Use this procedure to transfer an ISO image delivered through Electronic Software Delivery (ESD) from a customer drop box to a Succession Server Platform Foundation Software (SSPFS)-based server, and mount it onto the SSPFS-based server.

This procedure is applicable to software loads for the CS 2000 Management Tools (CS2M) component.

Note: The ESD software is formatted as an ISO 9660 image.

Prerequisites

This procedure has the following prerequisites:

- Your operating company must have an ESD agreement with Nortel Networks. When the agreement was established, the operating company provided Nortel Networks with the location of a drop box and a user name and password pair for delivering software loads. When Nortel Networks delivers a software load to the drop box, an electronic mail notification is sent to the e-mail address specified by the operating company when the ESD agreement was established.

  Note: For more information about ESD, refer to the Electronic Software Delivery Customer Implementation Guide.

- The SSPFS has been upgraded. If required, refer to procedure "Upgrading SSPFS Software" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server to which you want to transfer the software load

2 When prompted, type your user ID and password, and press the Enter key.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, type the root password and press the Enter key.

5 Ensure enough disk space is available for the ESD software by typing

```
# df -k /
```

and pressing the Enter key.

Note: It is recommended to have a minimum of 800 MByte of available disk space.

Example response

```
# df -k /
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d2         3082223  144125 2876454    5%    /
```

2876454 / 1000 = 2876 MB free

The value under the avail column is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes.

6 Transfer the ESD software load from the drop box on the repository server to the SSPFS-based server as follows:

a Access the repository server through FTP by typing

```
# ftp <repository_server>
```

and pressing the Enter key.

where

<repository_server>
is the machine owned by the operating company that was selected to be the destination for ESD software.

b Log in and change directory to the drop box location on the repository server.

c Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

d List the contents of the drop box by typing

```
ftp> ls
```

and pressing the Enter key.

e Transfer the ESD software load onto the SSPFS-based server by typing

```
ftp> get <iso_image>
```

and pressing the Enter key.

where

<iso_image>
is the CS2M ISO image filename for the software load

Example
ftp> get CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz

f Uncompress the software load file.

```
gzip -d  CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar.gz
```

g Untar the software load file.

```
tar -xvf  CS2M0080.80.P.NCL.NAP.VAULT.1.D.tar
```

h Access the directory that contains the software load file by typing

```
cd  CS2M0080.80.P.NCL.NAP.VAULT.1.D
```

and list the file in the directory.

i Change the name of the file in the directory by typing

```
mv CS2M0080_load.iso.tape CS2M0080_load.iso
```

j End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

7 Mount the ISO image as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

b Enter the number next to the “Other” option in the menu.

Example response

```
Other
 1 - Log Rotation
 2 - capt_files (Capture Various SSPFS
     Files/Logs For Debugging Purposes)
 3 - sun_explorer (Execute the Sun Explorer
     Data Gathering Tool)
 4 - mount_image (Mount A Generic Iso Image
     To The SSPFS Unit)
 5 - umount_image (Un-Mount A Generic Iso
     Image From The SSPFS Unit)


 X - exit

select -
```

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

If the response is	Do
`Enter the full path of the ISO image`	substep e
`ISO Image Already Mounted`	substep d

d Enter the number next to the “umount_image” option in the menu and retry substep c.

Note: If the umount_image or mount-image command is unsuccessful a second time, contact your next level of support.

e When prompted, type the full path name of the ISO image on the server from the root and press the Enter key.

The contents of the ESD software file are placed in directory /tmpmnt.

Note: Do not attempt to access the /tmpmnt directory until the mount command is complete.

If the response is	Do
`Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you umount an image before removing the image file. If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit`	step f
`Provided full path to ISO image does not exist`	verify the location and name of the ISO 9660 image
`Error creating the image device location`	This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact your next level of support.
`ERROR MOUNTING <ESD_filename>`	This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt` directory has been deleted. Repeat this procedure, and if it fails a second time, contact your next level of support.

f Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

8 You have completed this procedure. Proceed to upgrade the software using the relevant procedure.

Unmount and remove an ISO image from an SSPFS-based server

Application

Use this procedure to unmount and remove an ISO image delivered through Electronic Software Delivery (ESD) from a Succession Server Platform Foundation Software (SSPFS)-based server.

This procedure is applicable to software loads for the following components:

- Gateway Controller (GWC)
- CS 2000 Management Tools (CS2M)
- Audio Provisioning Server (APS)
- Integrated Element Management System (EMS)

Prerequisites

The component has been upgraded.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the SSPFS-based server on which the software you want to unmount and remove resides

2 When prompted, type your user ID and password, and press the Enter key.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, type the root password and press the Enter key.

5 Unmount the ISO image as follows:

a Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select -
```

b Enter the number next to the “Other” option in the menu.

Example response

```
Other
 1 - Log Rotation
 2 - capt_files (Capture Various SSPFS
     Files/Logs For Debugging Purposes)
 3 - sun_explorer (Execute the Sun Explorer
     Data Gathering Tool)
 4 - mount_image (Mount A Generic Iso Image
     To The SSPFS Unit)
 5 - umount_image (Un-Mount A Generic Iso
     Image From The SSPFS Unit)


 X - exit

select -
```

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

d Exit each menu level of the command line interface to eventually return to the root level prompt, by typing

`select - x`

and pressing the Enter key.

6 Remove the ISO image from the server by typing

`# rm /<loadname>`

and pressing the Enter key.

You have completed this procedure.

Create a backup of the GWC load file

Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a copy of one or more existing GWC load images stored on the CS 2000 Core Manager or CBM.

When to use this procedure

Use this procedure prior to saving an image of a GWC load if you wish to save a backup of the original GWC load stored on the CS 2000 Core Manager or CBM.

Note: If a backup is not created, then the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM.

Prerequisites

There are no prerequisites to this procedure.

Action

At the CS 2000 Core Manager or CBM console

1 Log in to the CS 2000 Core Manager or CBM as the root user.

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

2 Change directory to the GWC software directory by typing

 # cd /swd/gwc

and pressing the Enter key.

3 Type **ls** and press the Enter key to list the contents of the directory.

4 Locate the load file name that corresponds to the load you wish to back up.

Note: There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of a specific GWC card or node, refer to procedure "View the operational status of a GWC" found in *Gateway Controller Configuration Management*, NN10205-511, to locate the load filename associated with a specific GWC card.

5

CAUTION

Be sure to use the command **cp** in this step.

Failure to use the **cp** command can cause problems with the general upgrade process.

Make a copy of the existing GWC software load file by typing

 # cp <load_filename>.imag <load_filename>.imag.bak

and pressing the Enter key.

where

<load_filename>
is the GWC load filename that you want to copy

Note: You can use any name for the backup file name. You can also include the date in this filename, for example: <load_filename>.imag.031201

6 Change the permissions for the image file by typing

 # chmod 755 <load_filename>.imag.bak

and pressing the Enter key.

where

<load_filename>
is the GWC load filename

7 This procedure is complete.

Note: To return to the procedure that sent you here, refer to "Overall GWC upgrade procedure" (automated or manual) in *Upgrading the Gateway Controller*, NN10196-461.

View the contents of a load file image

Purpose of this procedure

This procedure allows you to view the content of the current load file located on the CS 2000 Core Manager or Core and Billing Manager (CBM). You can view the list of patches that have been applied and activated on the load file image. A load file is created by taking an image of a software load present on a GWC device. You may take an image manually or automatically.

Note: Perform this procedure on the CS 2000 Management Tools server since the gwclfinfo command is a SESM script, and the /swd/gwc load directory is NFS-mounted on the CS 2000 Management Tools server as /var/opt/nortel/gwc directory.

When to use this procedure

Use this procedure to confirm the contents of a load file image on the CS 2000 Core Manager or CBM before rebooting GWC devices from the file.

Use this procedure to determine if delivered load contains patches.

Prerequisites

This procedure has no prerequisites.

Action

Use the following table to determine your first step.

If your office has	Do
a CS 2000 Core Manager installed	go to step 1
a CBM installed	go to step 5

At the CS 2000 Management Tools server

1 Access the directory where the GWC load file information is located by typing

```
# cd /var/opt/nortel/gwc
```

and pressing the Enter key.

2 List all the GWC load names by typing

```
# ls
```

and pressing the Enter key.

3 Select the new GWC software load from the list and display its content by typing

 # /opt/nortel/NTsesm/tools/gwc_tools/ gwclfinfo /var/opt/nortel/gwc/<gwc_load_file>

and pressing the Enter key.

where

<gwc_load_file>
is the name of the selected GWC load image file, for example pgc09bl_patched_03_04.imag

Note: In the above command, insert a space after the "gwclfinfo" character string. Do not insert any other spaces.

Example response:

```
Load information from pgc09bl_patched_03_04.imag

Load name: PGC09BL Image created: Fri Mar 5 7:0:21 2004

Patch-ID    Status    Activation
XBN63GZ9    Applied   NonAct
XED41GZ9    Applied   NonAct
XQA89GZ9    Applied   NonAct
.
.
.
```

4 This procedure is complete.

Note: To return to the procedure that sent you here, refer to "Overall GWC upgrade procedure" (automated or manual) in *Upgrading the Gateway Controller*, NN10196-461.

At the CS 2000 Management Tools terminal

5 Access the temporary directory by typing

 # cd /tmp

and pressing the Enter key.

6 Access the CBM server by typing

 # ftp <CBM_IP_address>

and pressing the Enter key.

where

<CBM_IP_address>
is the IP address of the CBM server

7 When prompted, enter the user name by typing

Name: gwcload

and pressing the Enter key.

8 When prompted, enter the password by typing

Password: gwcload

and pressing the Enter key.

9 Set up the ftp transfer process to binary by typing

ftp> bin

and pressing the Enter key.

10 Transfer the GWC image load file by typing

ftp> get <gwc_image_name>

and pressing the Enter key.

where

<gwc_image_name>
is the name of the GWC load image file stored on the CBM server

Example response:

```
200 PORT command successful.
150 Opening data connection for pgt93ax.imag (binary mode
                                                (10294018).
226 Transfer complete.
local: pgt93ax.imag remote: pgt93ax.imag
10294018 bytes received in 5.3 seconds (1908.92 Kbytes/s)
```

11 Return to the /tmp directory on the CS 2000 Management Tools server by typing

ftp> quit

and pressing the Enter key.

12 Display the content of the GWC software load image by typing

 # /opt/nortel/NTsesm/tools/gwc_tools/gwclfinfo /tmp/<gwc_image_name>

and pressing the Enter key.

where

<gwc_image_name>
is the name of the transferred GWC load image file

Example response:

```
Load information from pgt93ax.imag

Load name: PGT93AX Image created: Fri Mar 5 7:0:21 2004

Patch-ID    Status    Activation
XBN63GZ9    Applied   NonAct
XED41GZ9    Applied   NonAct
XQA89GZ9    Applied   NonAct
.
.
.
```

13 When you are finished reviewing the content of the file, remove the GWC load image from the /tmp directory by typing

`# rm /tmp/<gwc_image_name>`

and pressing the Enter key.

where

`<gwc_image_name>`
is the name of the transferred GWC load image file

14 This procedure is complete.

Note: To return to the procedure that sent you here, refer to Overall GWC upgrade procedure (manual or automated) in *Upgrading the Gateway Controller*, NN10196-461.

Upgrade a standby GWC card software load

Purpose of this procedure

This procedure describes how to upgrade the software load that GWC cards boot from, located on the CS 2000 Core Manager or Core and Billing Manager (CBM).

When to use this procedure

Use this procedure after installing a newer version of the GWC software load onto the CS 2000 Core Manager or CBM. This procedure must be applied to each node installed in the SAM21 shelf that is being upgraded.

Prerequisites and guidelines

CAUTION

No provisioning activity can occur on the system while the GWC software upgrade is in progress.

The GWC software load filesets must be installed on the CS 2000 Core Manager or CBM. Refer to one of the following procedures:

- Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 69
- Transfer and mount an ISO image delivered through ESD onto an SSPFS-based server on page 75

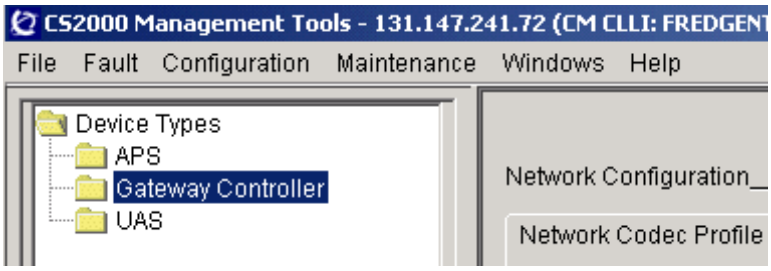
While upgrading the software on a GWC card, the port on the LAN router connected to the GWC card must be set to the Ethernet parameter of “auto-negotiate”. This action must be performed after the card is locked and before the card is unlocked. Refer to step 9 in this procedure.

If the Communications Server LAN (CS LAN) is provided by Nortel Networks Ethernet Routing Switch 8600 routers, refer to Re-provision Ethernet Routing Switch 8600 port to auto-negotiate on page 105 for a procedure to reconfigure the port on the CS LAN router to “auto-negotiate”.

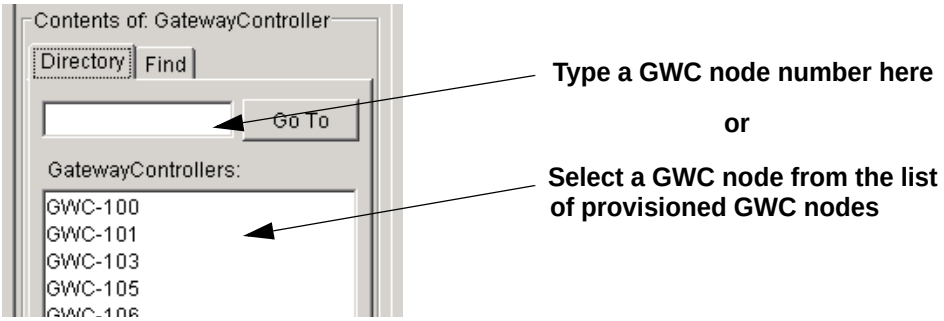
Action

At the CS 2000 GWC Manager client

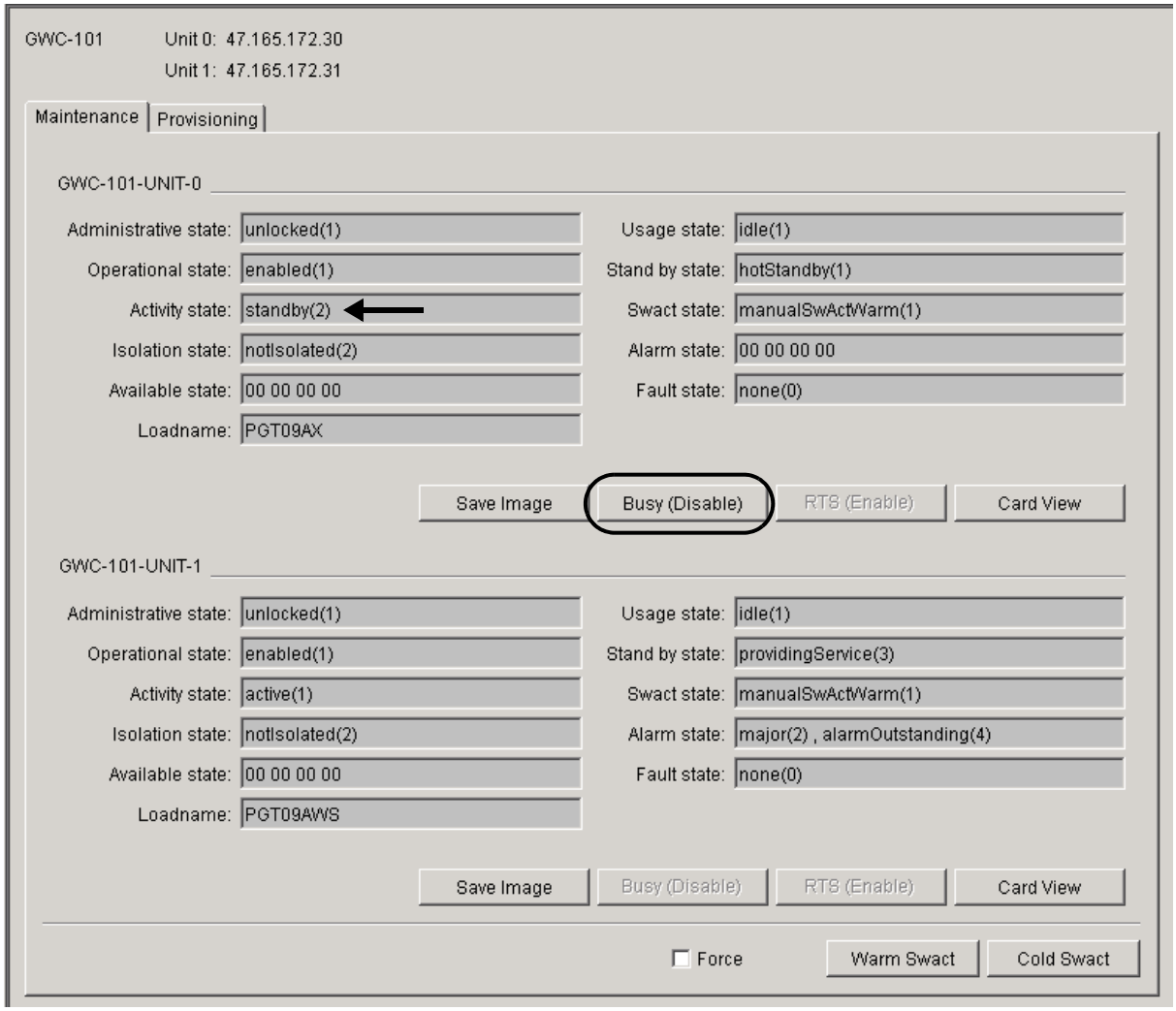
1 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



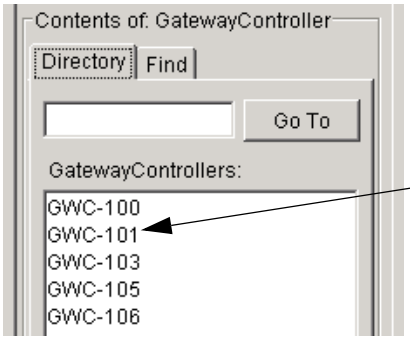
2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to busy for an upgrade.



3 Busy the standby GWC card in the node to upgrade by clicking the **Busy (Disable)** button. Confirm this action at the prompt.



4 From the Contents of: Gateway Controller record the GWC node number for the GWC card you just busied. You will need this information later in this procedure.



Record the GWC node number of the GWC card that you just busied.

5 Use the following table to determine your next step.

If	Do
you need to re-provision the port on the Ethernet Routing Switch 8600 to "auto-negotiate" (the CS LAN is provided by Ethernet Routing Switch 8600 routers)	go to step 6
otherwise	go to step 7

At the CLI for the Ethernet Routing Switch 8600

6 Determine the slot and port on the router that connects to the device by typing

> show ip arp info <ip_address>

and pressing the Enter key.

ip_address
is the physical IP address of the GWC card.

The slot and port are reported. Record the slot and port number. You will need this information later in this procedure.

Example response:

```
prompt:cpu> show ip arp info 172.30.242.25
================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
172.30.242.25    00:90:69:1a:d4:fc   200   1/2   DYNAMIC 272
```

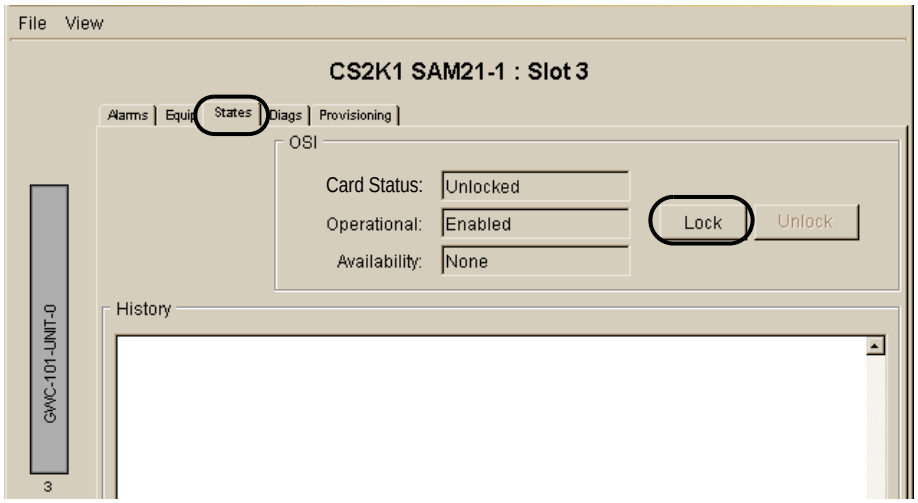
Note: *If the response indicates MLT instead of the slot and port, perform this operation from the mate router unit. If the response indicates that no arp entry is found, ping the IP address from the CLI, and retry the command.*

At the CS 2000 GWC Manager client

7 Click the **Card View** button for the card you busied in step 3. This action opens the CS 2000 SAM21 Manager.

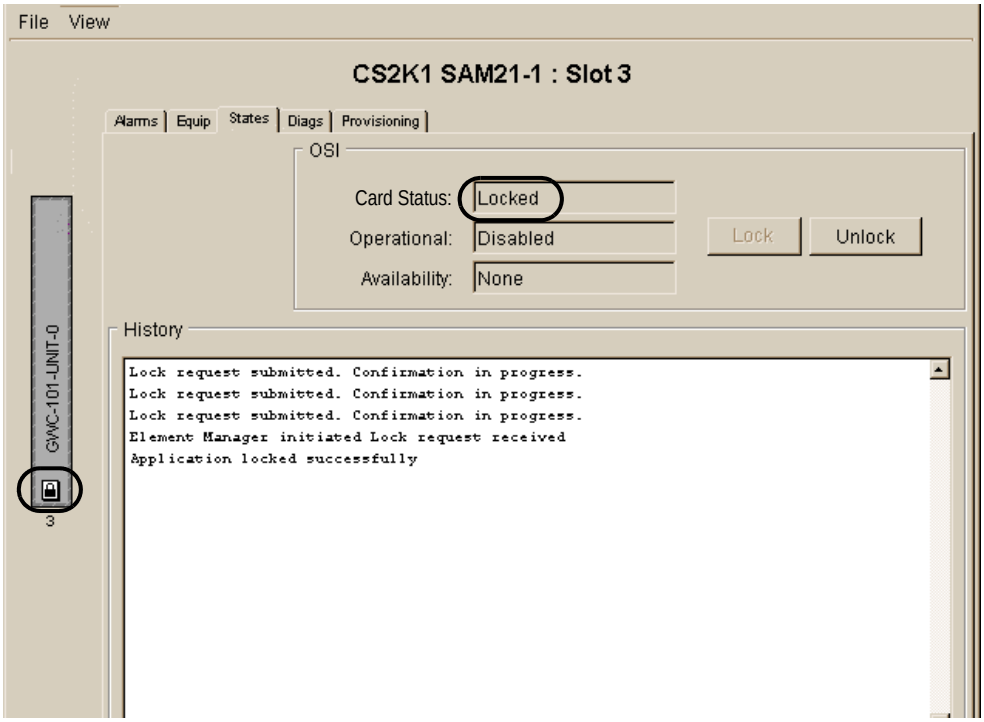
At the CS 2000 SAM21 Manager client

8 In the card view, select the **States** tab and then click the **Lock** button to lock the card.

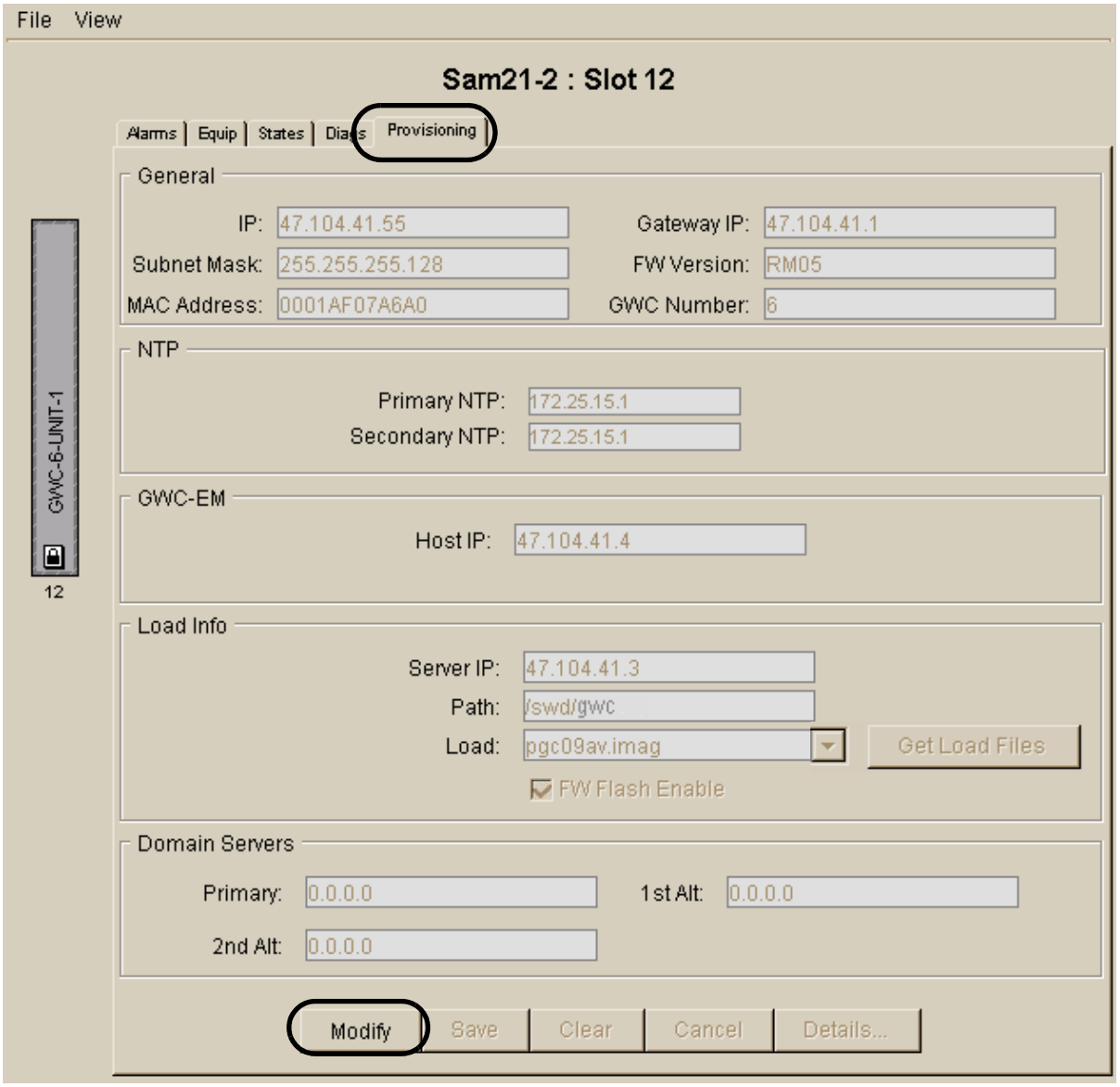


9 Observe the History display to confirm that the card has been locked. Look for the text “Application locked successfully”. Also, notice the lock icon on the card graphic at the left of the screen and the Card Status “Locked”.

Note: If the CS LAN is provided by Ethernet Routing Switch 8600 routers, re-provision the port on the router switch to “auto-negotiate”. Refer to Re-provision Ethernet Routing Switch 8600 port to auto-negotiate on page 105.



10 Select the **Provisioning** tab and click the **Modify** button to change the load file name.



11

> **CAUTION**
>
> The Path: field must be set to /swd/gwc (for CS 2000 Core Manager) or /gwc (for CBM).
>
> Other processes are tied to this directory. For example, the GWC load delivery software places the load in the /swd/gwc directory. Also, GWC auto-imaging is a network file system (NFS) mount of the /swd/gwc directory.

Click the **Get Load Files** button and select the required load from the drop-down list.

Note: Ensure that the FW Flash Enable check box is selected.

12 Use the following table to determine your next step.

If	Do
field **GWC Number:** is blank or the current value of the field does not match the number recorded in step 4	go to step 13
otherwise	go to step 14

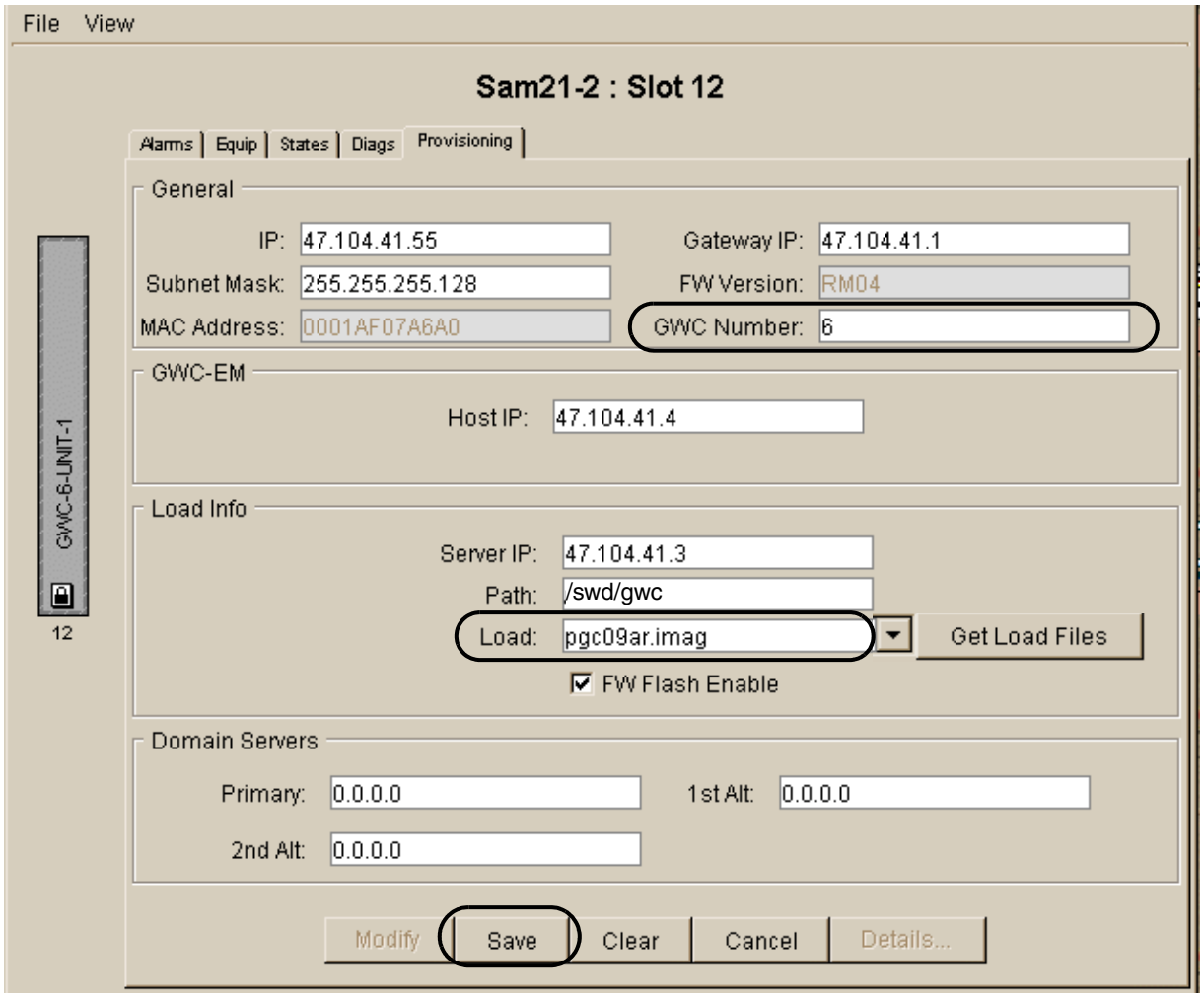
13 Type the GWC number in the **GWC Number:** field that you recorded in step 4. Refer to the following figure to locate these fields.

Note: Beginning in SN05 and going forward, there is a requirement to enter the GWC number into this field which is used to label the GWC in the CS 2000 SAM21 Manager shelf view panel. This number is manually assigned and no error checking is performed to ensure it matches with the number in the CS 2000 GWC Manager. A number from 0 to 255 can be assigned for each GWC pair in the node.

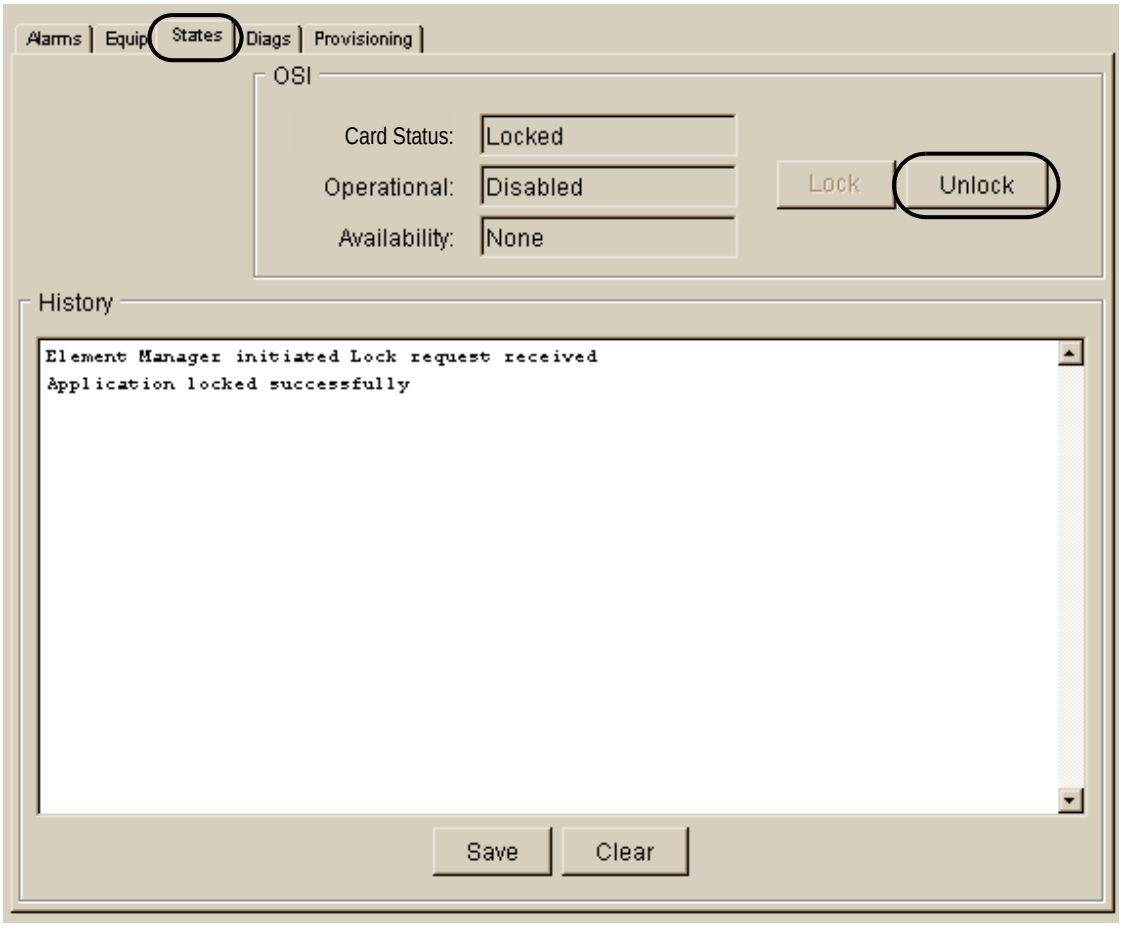
For example, if GWC cards in shelf slots 1 and 2 are paired together as a node, then during provisioning of these cards, the number 0 could be entered for each of these cards to identify that cards in slots 1 and 2 belong to GWC 0. Ensure that the GWC number entered at the CS 2000 SAM21 Manager matches the value given the cards in the CS 2000 GWC Manager as described in step 4.

14 Click the **Save** button.

Note: If the load name or path name are incorrect, you will be prompted with a “Load Validation Failure” message. You can choose to force the change or return to the provisioning panel to correct the error.



15 Click the **States** tab to display the status of the GWC card.

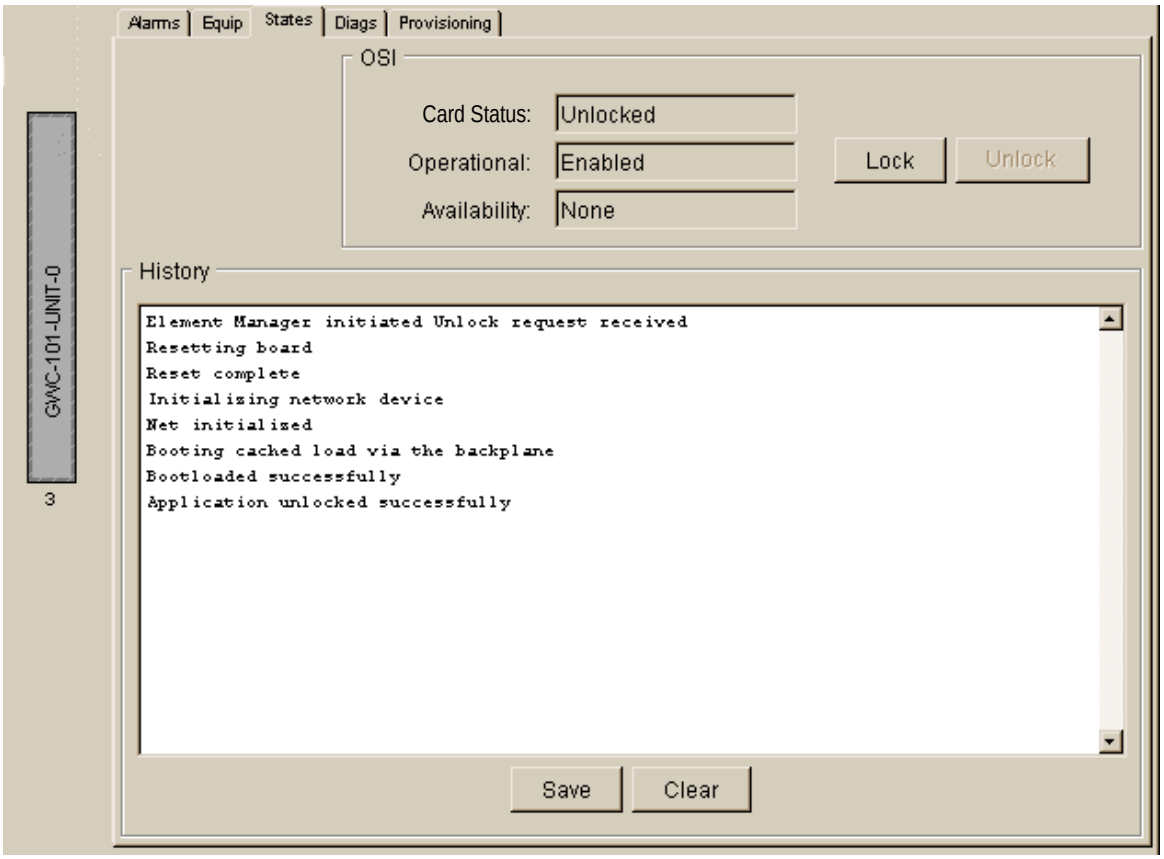


16 Click the **Unlock** button to unLock the “Inactive” GWC card. This causes the card to reset and load from the new load image. The inactive unit should automatically return to service (RTS).

17 Observe the History display until the screen message “Bootloaded successfully” appears.

Note: If the card status does not display “Application unlocked successfully”, then click the **Lock** button in the card view and wait for the “Application locked successfully” message. Then, click the **Unlock** button again.

If you are still unable to successfully unlock a GWC card, contact your next level of support.



At the CS 2000 GWC Manager

18 Use the following table to determine your next step.

If	Do
you are upgrading the first card in the seed GWC node, and there are patches that must be applied	go to step 19
otherwise	go to step 21

19 Patch the seed GWC unit by completing the tasks listed in the following table.

All necessary procedures, as well as the patching checklist and additional patching information, are available in the "Carrier Voice over IP Network patching" section of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Note 1: Apply all Released (R) and Propagated (P) status patches, take the image, and then apply Verification (V) status patches. It is best not to have V status patches in a saved image since these patches are normally applied to only one GWC.

Note 2: Apply all patches, including the ACT category patches that apply to your site. Contact Nortel Networks customer support to determine which ACT category patches must be activated in your site. Do not activate any other GWC ACT category patches unless advised to do so by Nortel Networks customer support.

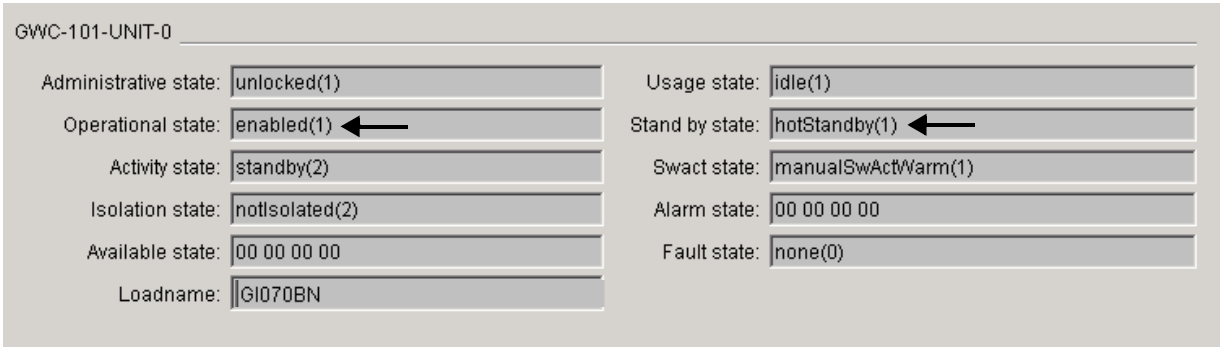
Task	Procedure
Audit the GWC unit for existing patch activity.	"Performing a device audit using the NPM"
Retrieve the patch files from CD or electronically, and copy them into the NPM database.	"Transferring patches to the NPM database manually"
If you wish, define reports for a GWC.	"Defining reports using the NPM"
Apply patches to the standby GWC unit.	"Applying patches using the NPM".

Task	Procedure
Activate the applicable patches.	“Activating patches using the NPM”
If required, deactivate any obsolete patches.	“Deactivating patches using the NPM”
If required, remove any obsolete patches.	“Removing patches using the NPM”

20 Take an image of the standby GWC unit. Follow procedure Take a manual GWC software image on page 119.

21 Verify that the inactive GWC has an Operational State of “enabled” and a standby state of “hotstandby”.

If the inactive GWC does not come into an Operational State of “enabled” and a Standby state of “hotstandby”, then refer to the section “GWC does not RTS” in the procedure Troubleshoot GWC upgrades on page 141 in this NTP. If error recovery fails, stop this procedure and contact your next level of support.

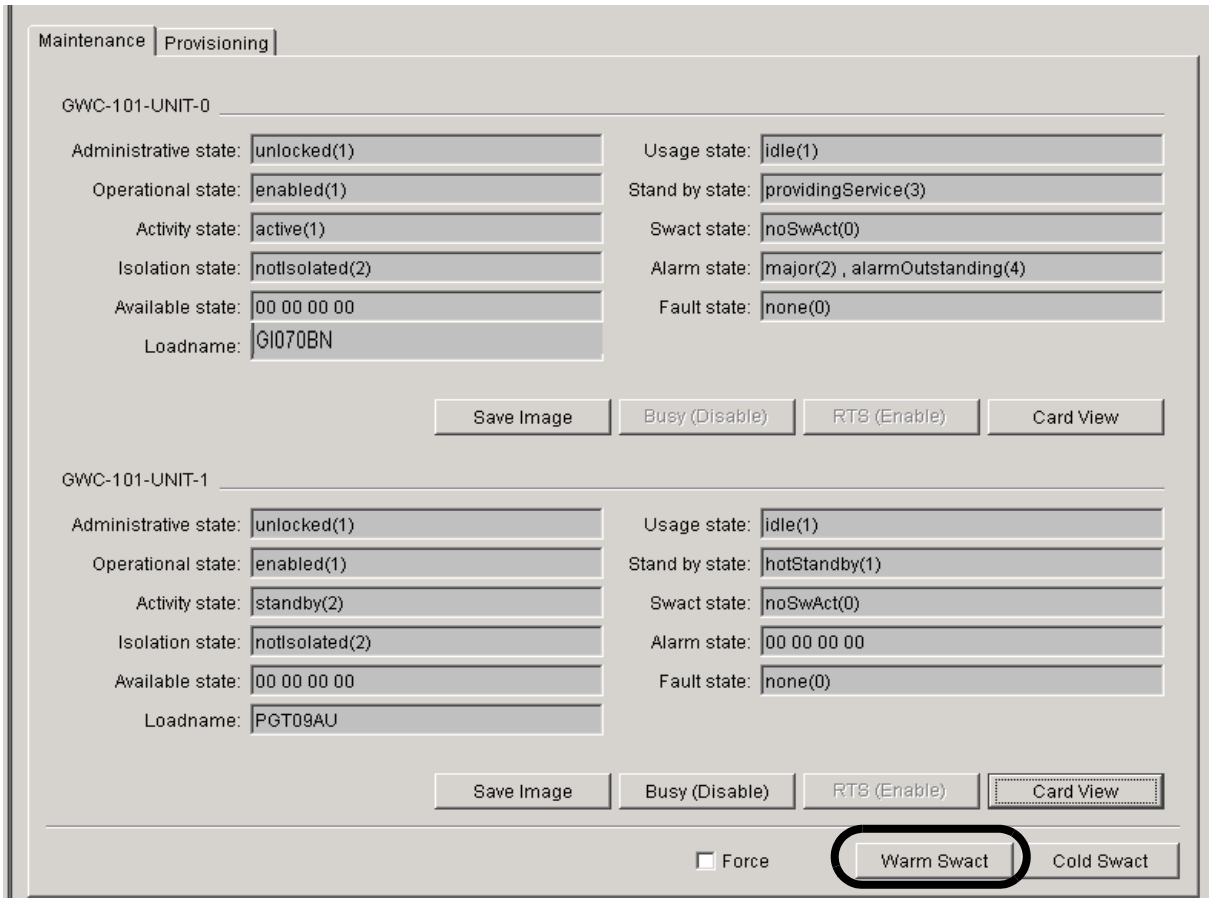


At the CS 2000 GWC Manager

22 Perform a Warm SwAct by clicking the **Warm Swact** button.

Note: If the SwAct fails or the inactive unit does not RTS in 1 minute, then refer to the section “Warm SwAct Failed” in the procedure Troubleshoot GWC upgrades on page 141 in this NTP.

If the GWC card does not successfully execute a warm SwAct using the Troubleshooting procedure, then perform the procedure Roll back a software upgrade on a GWC node on page 107 in this NTP.



23 Use the following table to determine your next step.

If	Do
you need to upgrade the mate GWC card (now the new standby GWC card) in the same node	go to step 3 and complete this procedure
you need to upgrade cards in another GWC node	go to step 2 and complete this procedure
all cards in all GWC nodes have been upgraded[1]	go to step 24

1. You need to perform this procedure only once for each card in each GWC node.

24 This procedure is complete.

Note: To return to the Overall manual GWC upgrade procedure, refer to Overall upgrade process - manual on page 65.

Re-provision Ethernet Routing Switch 8600 port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Ethernet Routing Switch 8600.

Note: Make sure you use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to the Ethernet Routing Switch 8600 documentation and choose Getting Started.

At the CLI for the Ethernet Routing Switch 8600

1 Use the numbers recorded in step 6 and set the slot and port to auto-negotiate by typing

> config ethernet <slot>/<port> auto-negotiate enable

and pressing the Enter key.

The slot and port are reconfigured to auto-negotiate and the prompt returns.

```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

2 Verify the port configuration by typing

> show ports info config <slot>/<port>

and pressing the Enter key.

The slot and port configuration is displayed.

```
prompt:cpu> show ports config info 1/2

================================================================================
                                    Port Config
================================================================================

PORT                 AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT
NUM   TYPE           NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID
--------------------------------------------------------------------------------
1/2   100BaseTX      true  false  half  100   full  100   fals  core  1   0
```

3 Commit the change by typing

> save config

and pressing the Enter key.

4 Go to step 10 to continue with the procedure “Upgrade a standby GWC card software load”.

Roll back a software upgrade on a GWC node

Purpose of this procedure

This procedure describes how to roll back a software upgrade and revert to a previous software load.

When to use this procedure

Use this procedure when a software upgrade fails.

CAUTION

Downgrades are only supported as part of backing out of the upgrade of an individual GWC type. Call survivability, as specified in the service impact matrix in section Upgrade and downgrade call service impact on page 16, is not supported for downgrades once further non-GWC network components have been upgraded or further GWC types have been upgraded. This is especially problematic if the call server or gateways have already been upgraded. Call survivability support during downgrades is limited only to backing out of all instances of the last GWC card type that was being upgraded.

Prerequisites

The following prerequisites apply to this procedure:

- A GWC software load file from a previous release or a backup image file must be available on the CS 2000 Core Manager or Core and Billing Manager (CBM).
- If your system contains shared network address translators (NAT) with manually assigned zone ID, you must delete all instances of these NATs before downgrading to a software load earlier than SN07. Refer to procedure “Delete a network service zone” in *Gateway Controller Configuration Management*, NN10205-511.

- If you suspect that the call agent ID for your CS 2000 has ever been changed, contact Nortel Networks customer support before attempting to roll back to a software load earlier than SN07.

CAUTION

Active calls on the GWC node affected may be dropped during a software rollback. Ensure that all steps in this procedure are followed to minimize the risk of calls being dropped.

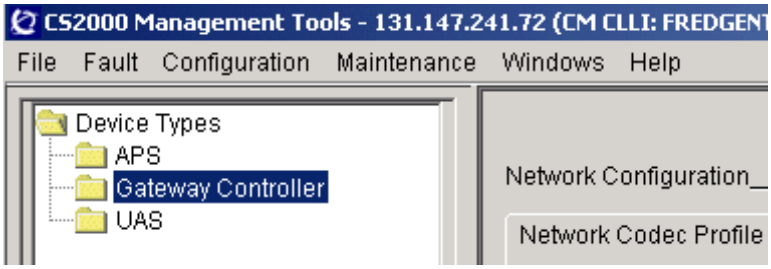
CAUTION

No provisioning activity can occur on the system while the GWC software downgrade is in progress.

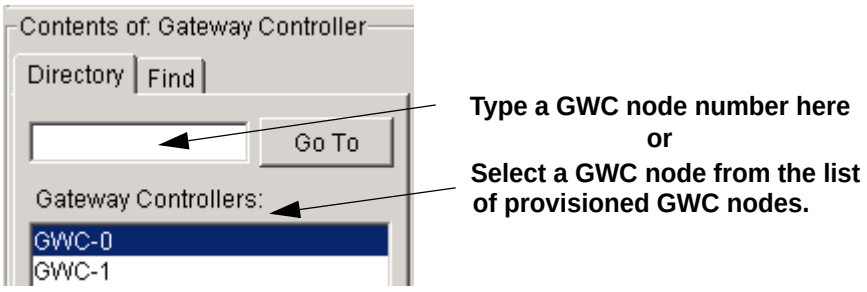
Action

At the CS 2000 GWC Manager client

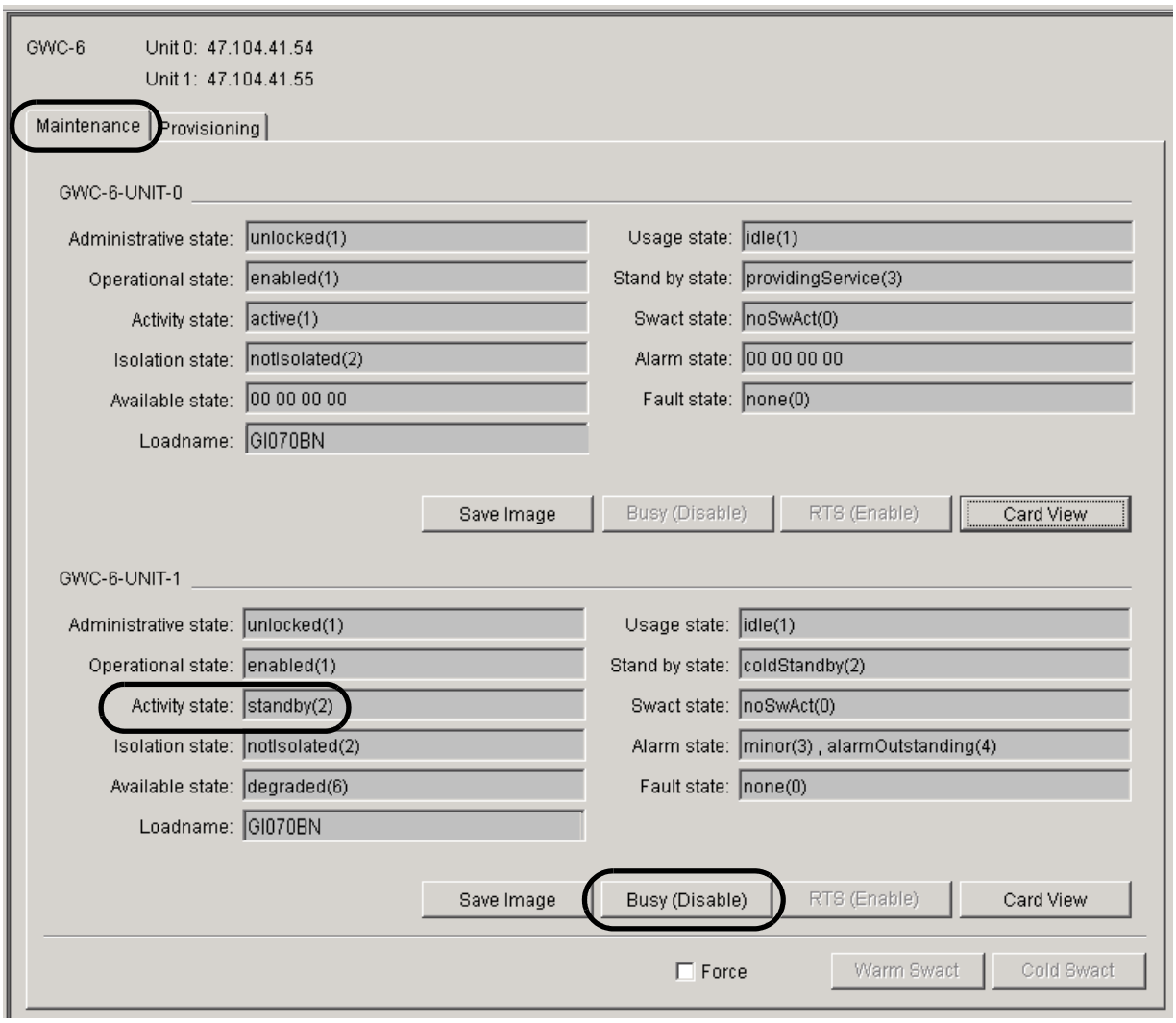
1 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



2 From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to roll back.



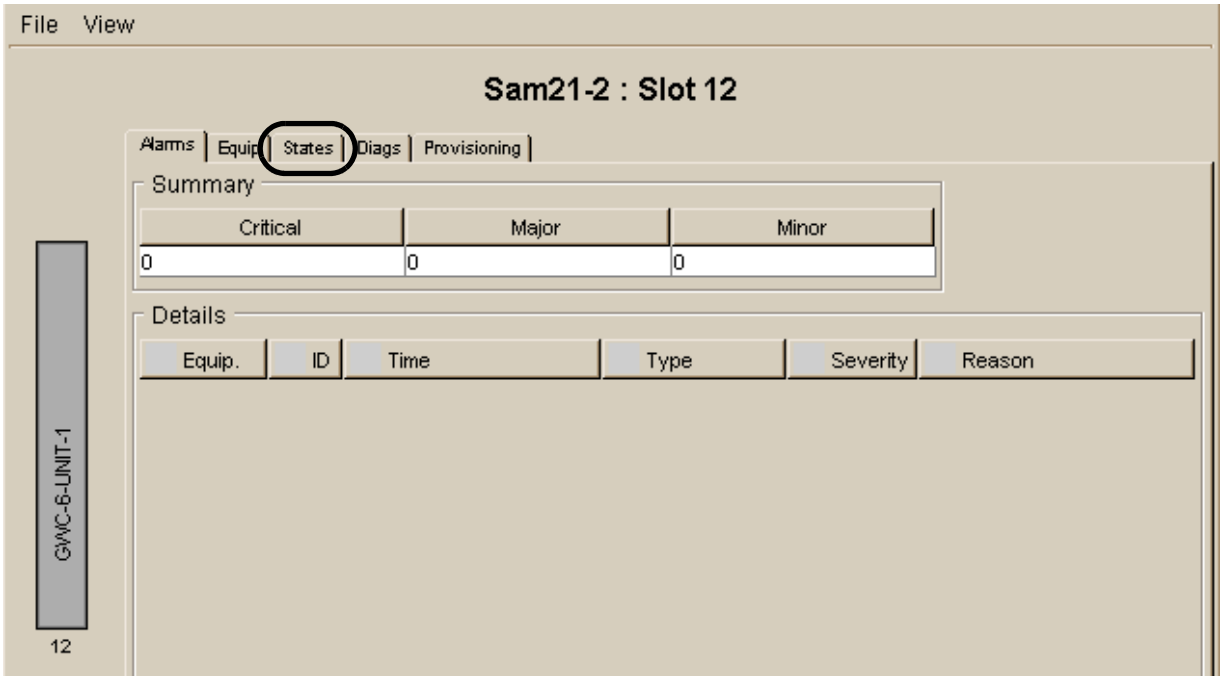
3 Rollbacks can only occur on a standby GWC card. Select the **Maintenance** tab and locate the standby card. Busy the standby GWC card by clicking the **Busy (Disable)** button and confirm this action at the prompt.



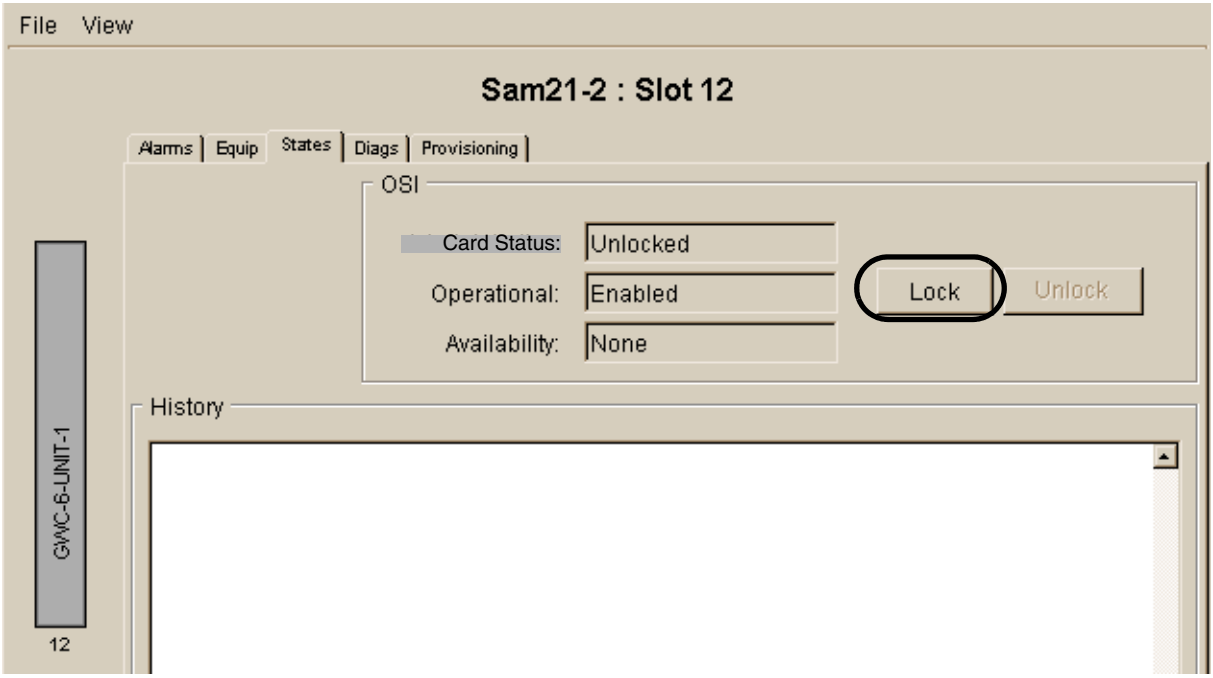
4 When the Operational state of the standby card is disabled, click the **Card View** button to access the card view. This action opens the CS 2000 SAM21 Manager.

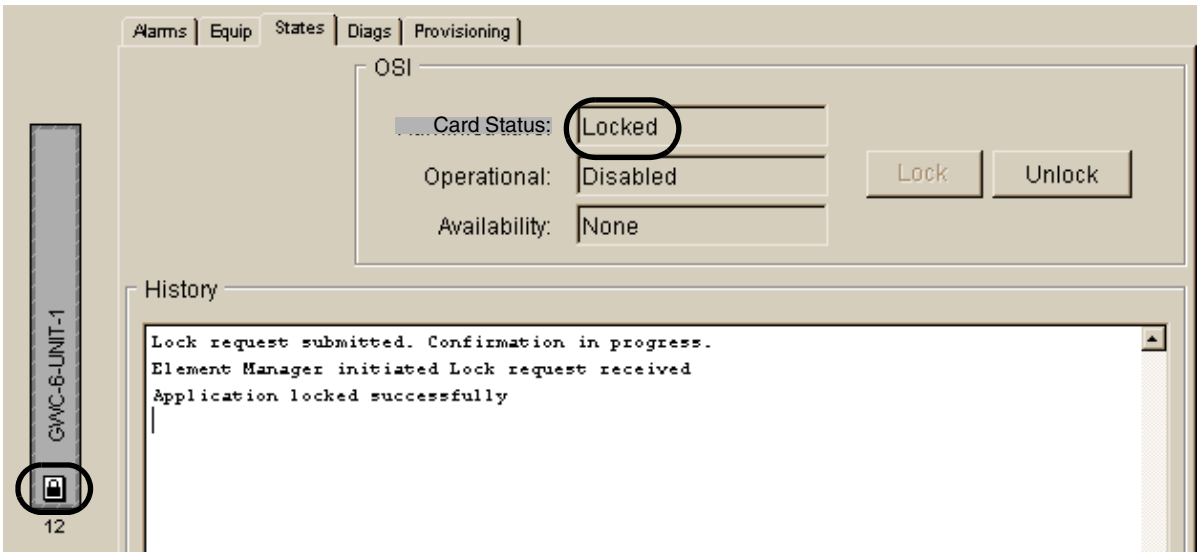
At the CS 2000 SAM21 Manager client

5 Select the **States** tab in the card view.

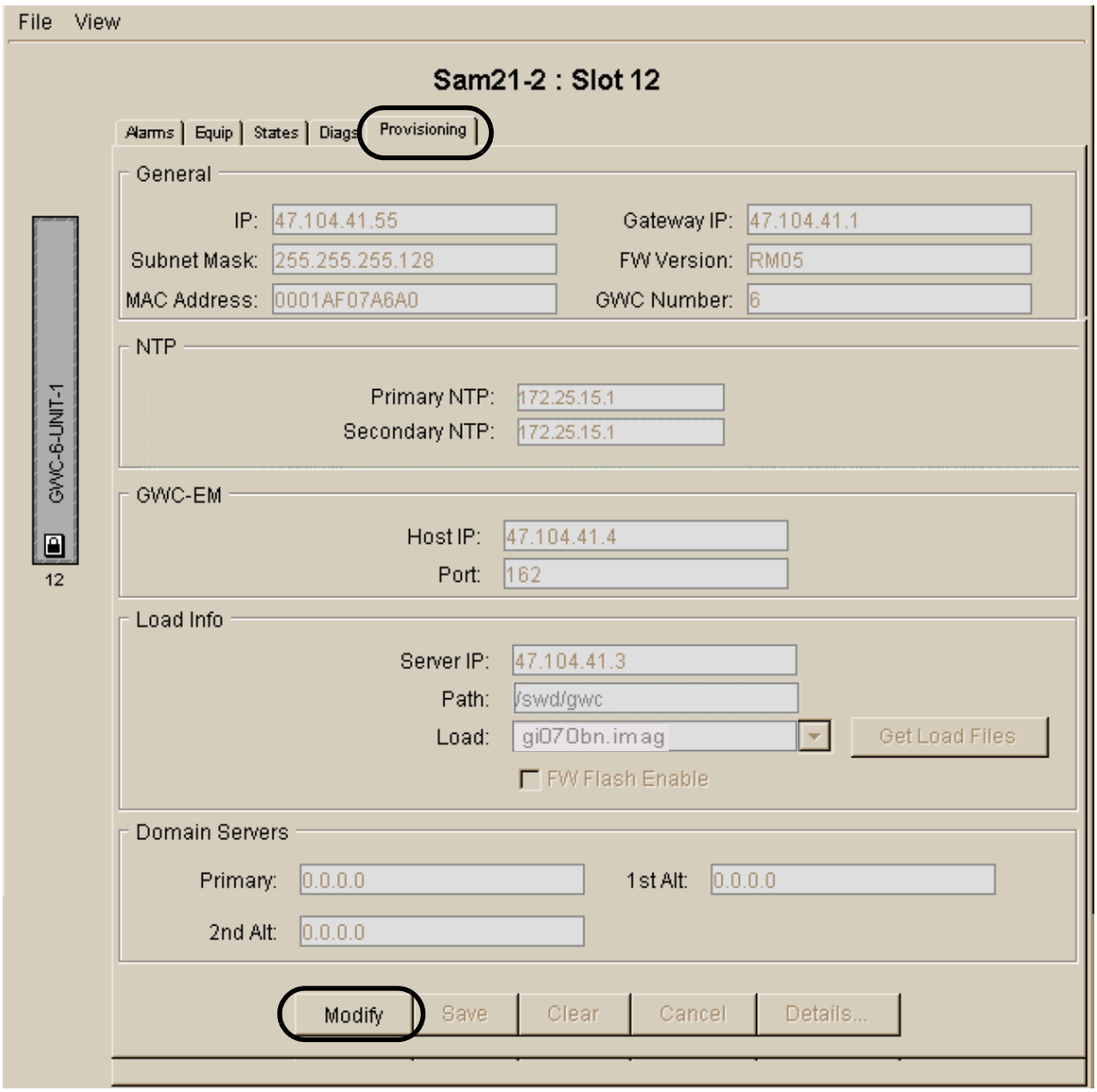


6 Click the **Lock** button to lock the card. Wait for the message in the History window indicating that the card is locked. Also, notice the lock icon on the card graphic at the left of the screen and the Card Status “Locked”.





7 Select the **Provisioning** tab in the card view.



8 Click the **Modify** button to make changes to the provisioning datafill.

9 Click the **Get Load Files** button and select from the drop-down list the load to which you want to revert.

10

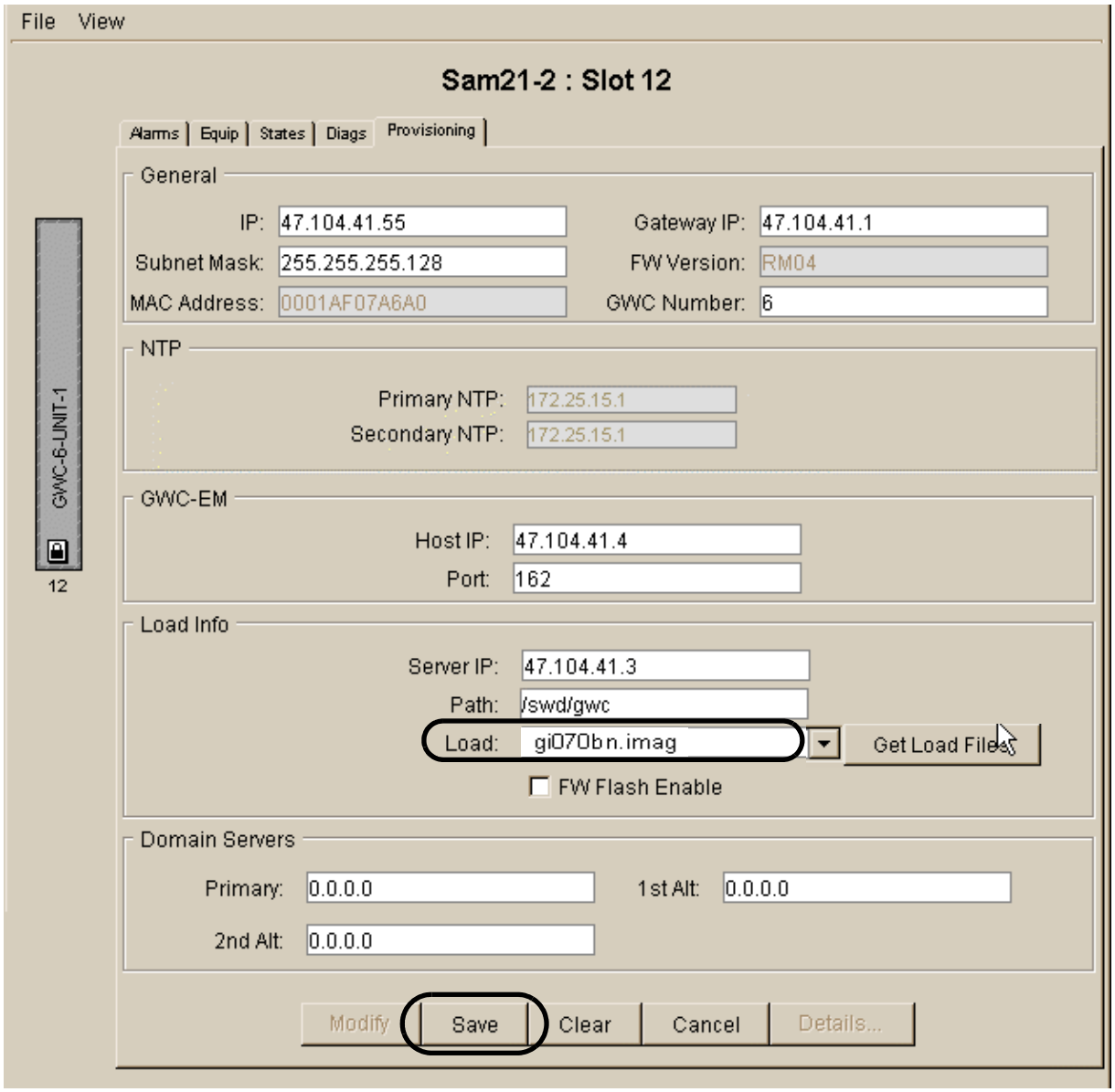
CAUTION

In this step, the Path: field must be set to /swd/gwc (for CS 2000 Core Manager) or /gwc (for CBM).

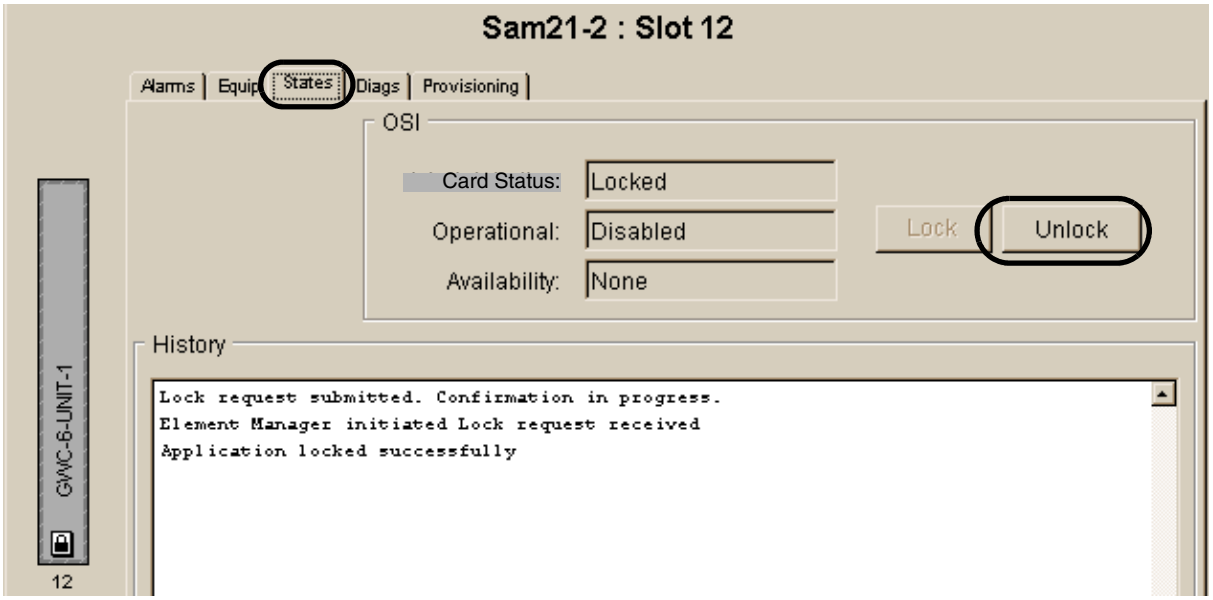
Other processes are tied to this directory. For example, the GWC load delivery software places the load in the /swd/gwc directory. Also, GWC auto-imaging is a network file system (NFS) mount of the /swd/gwc directory.

Click the **Save** button.

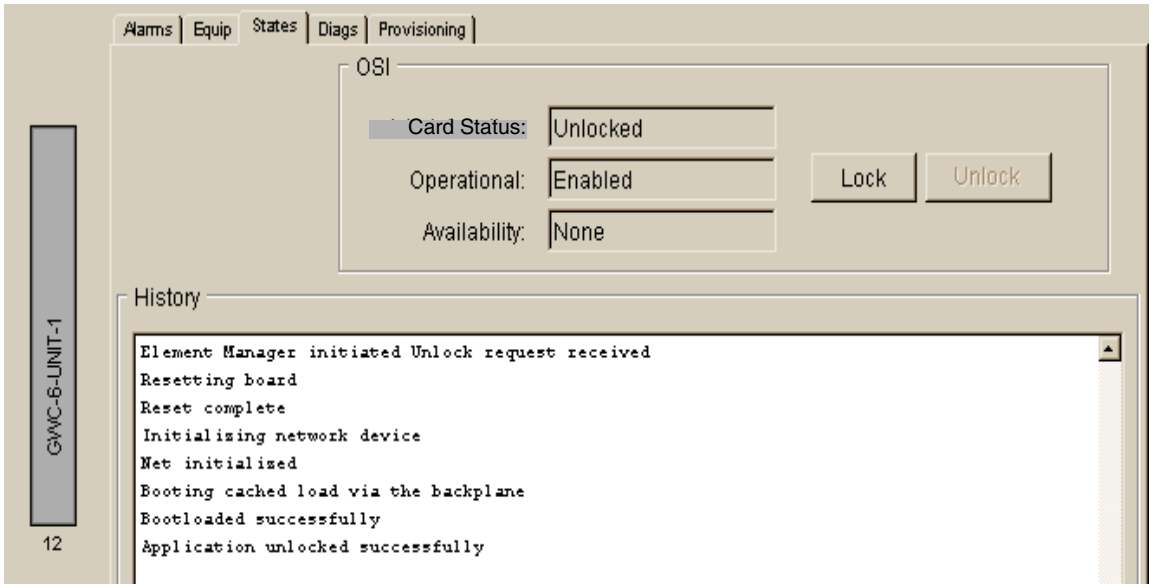
Note: Leave the FW (firmware) Flash Enable checkbox unselected.


File View
Sam21-2 : Slot 12
Alarms Equip States Diags Provisioning
GWC-6-UNIT-1
12
General
IP: 47.104.41.55
Gateway IP: 47.104.41.1
Subnet Mask: 255.255.255.128
FW Version: RM04
MAC Address: 0001AF07A6A0
GWC Number: 6
NTP
Primary NTP: 172.25.15.1
Secondary NTP: 172.25.15.1
GWC-EM
Host IP: 47.104.41.4
Port: 162
Load Info
Server IP: 47.104.41.3
Path: /swd/gwc
Load: gi070bn.imag
Get Load Files
FW Flash Enable
Domain Servers
Primary: 0.0.0.0
1st Alt: 0.0.0.0
2nd Alt: 0.0.0.0
Modify Save Clear Cancel Details...

11 Select the **States** tab in the card view.



12 Click the **Unlock** button to load the software you selected previously. Observe the History window display to confirm the the software reload was successful.



13 Use the following table to determine your next step.

If	Do
you are downgrading the first card in the seed GWC node, and there are patches that must be applied to the earlier software load[1]	go to step 14
otherwise	go to step 16

1.The image file of the earlier software load should already contain the required patches. The following steps to patch the load may not be required.

14 If necessary, patch the seed GWC unit by completing the tasks listed in the following table.

All necessary procedures, as well as the patching checklist and additional patching information, are available in the "Carrier Voice over IP Network patching" section of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

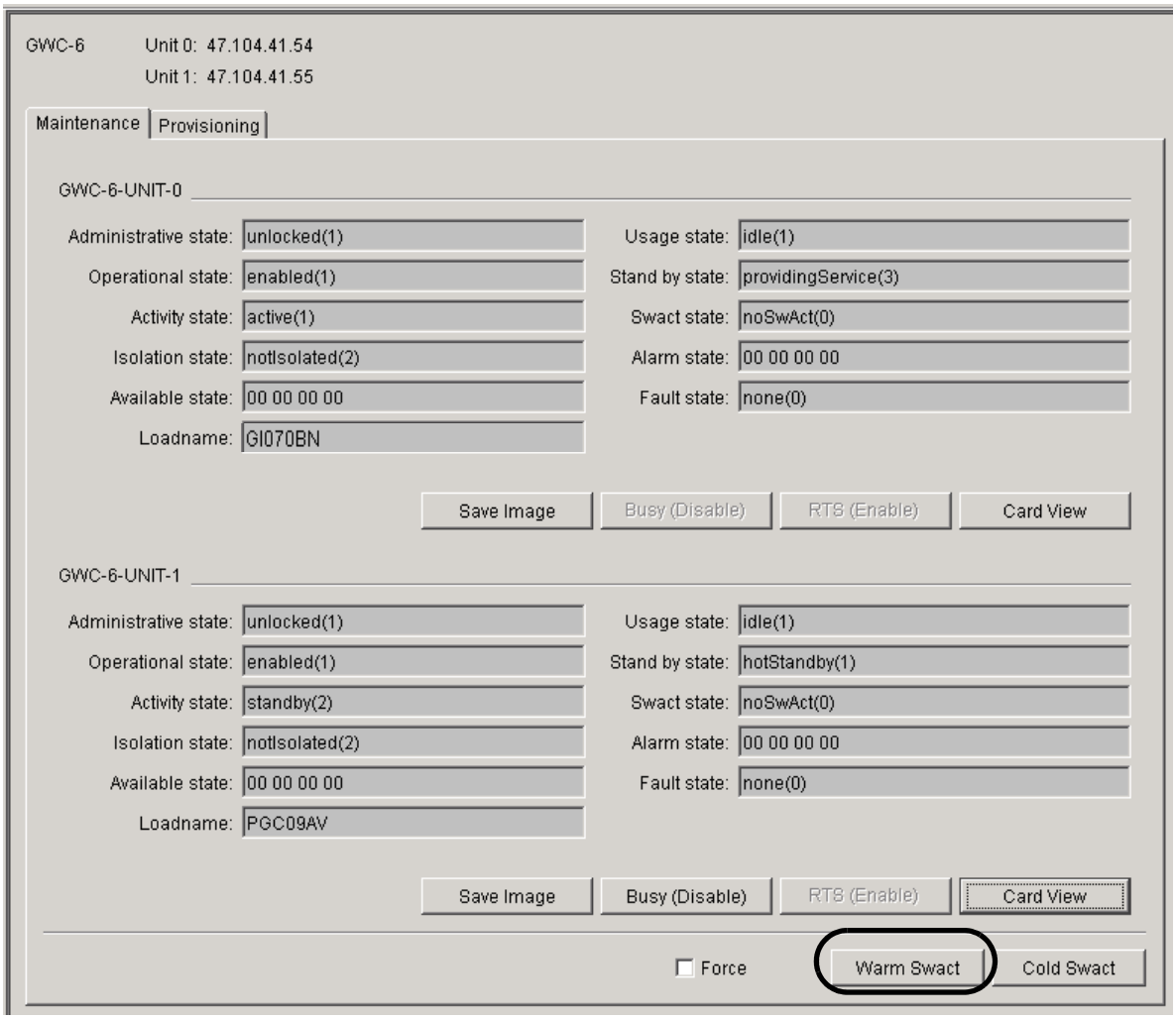
Task	Procedure
Audit the GWC unit for necessary patch activity.	"Performing a device audit using the NPM"
If you wish, define reports for a GWC.	"Defining reports using the NPM"
Apply patches to the standby GWC unit.	"Applying patches using the NPM".
Activate the applicable patches.	"Activating patches using the NPM"
If required, deactivate any obsolete patches.	"Deactivating patches using the NPM"
If required, remove any obsolete patches.	"Removing patches using the NPM"

15 Take an image of the standby GWC unit. Follow procedure Take a manual GWC software image on page 119.

At the CS 2000 GWC Manager client

16 Observe the Standby state field on the inactive GWC card in the Maintenance panel. Wait for the Standby state to transition from "coldStandby" to "hotStandby".

17 Apply a warm swact (switch of active cards) by clicking the **Warm Swact** button at the bottom of the screen.



18 Use the following table to determine your next step.

If	Do
you need to downgrade the mate GWC card (now the new standby GWC card) in the same node	go to step 3 and complete this procedure
you need to downgrade cards in another GWC node	go to step 2 and complete this procedure
all cards in all GWC nodes have been downgraded[1]	go to step 19

1. You only need to perform this procedure once for each card in each GWC node.

Note: Repeat this procedure for each GWC node until all units in each node are rebooted from the new image.

19 This procedure is complete.

Take a manual GWC software image

Purpose of this procedure

This procedure describes how to save a software image to the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

Note: A procedure also exists to enable the auto-imaging of a GWC software load once daily. Refer to Enable or disable GWC software auto-imaging on page 137 found in this NTP.

When to use this procedure

Use this procedure as a part of upgrading GWC software for an office or as a part of maintenance activity.

Take an image after all patches have been applied to GWC software. Refer to your site operating procedures for information about soak time and how many patches to apply before taking an image. In the absence of this information, Nortel Networks recommends taking an image immediately after applying R or P status patches.

CAUTION

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or incomplete image to be taken.

Prerequisites

This procedure has no prerequisites.

Action

At the CS 2000 Core Manager or CBM console

1 Log in to the CS 2000 Core Manager or CBM as the root user.

2 Change directory to the GWC software directory.

Example
 # cd /swd/gwc

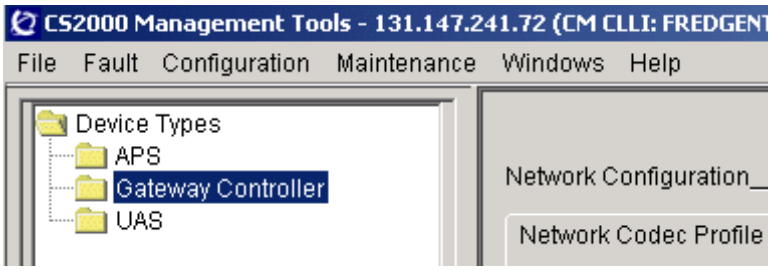
3 Copy the existing GWC software load file to a backup.

Example
 # cp pgc06as.imag pgc06as.imag.bak

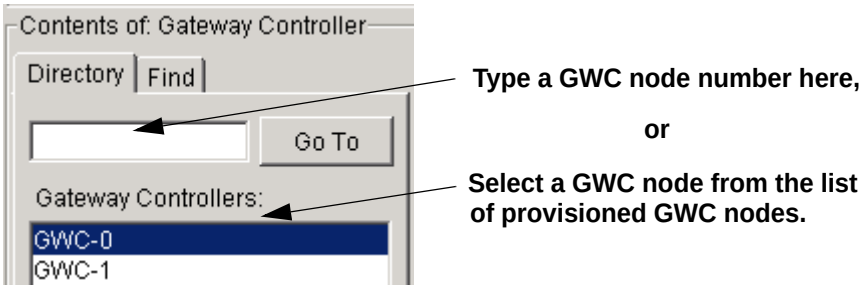
Note: You can use any name for the backup file name.

At the CS 2000 GWC Manager client

4 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



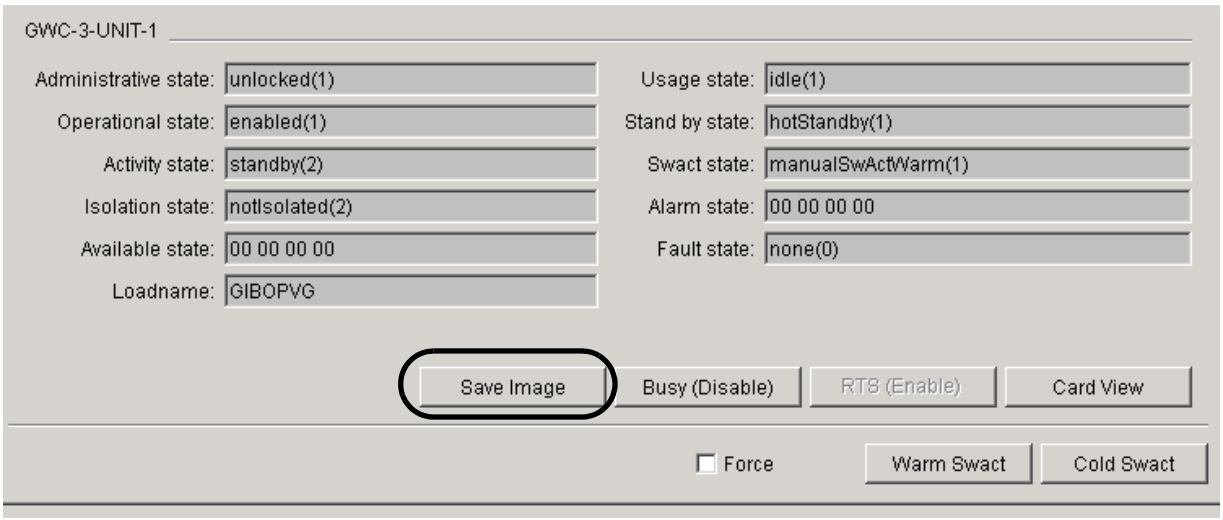
5 From the Contents of: Gateway Controller frame, select the appropriate GWC node from which you wish to take an image.



6 Select the **Maintenance** tab to view the Maintenance panel.

7 In the Maintenance panel, identify the GWC card in the node that has an upgraded load already installed.

a Click the **Save Image** button for that card to save the software image back to the CS 2000 Core Manager or CBM.



b At the following warning message, click **OK** to continue with saving the GWC card's software image on the CS 2000 Core Manager. To stop the operation, click **Cancel**.

Note: The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM. If the load file name is a link on the file system, the link is replaced with a file of the same name. Nortel Networks does not support using links to load files.

CAUTION

Do not invoke the Save Image function during patching activities. Doing so can cause an invalid or or corrupt image to be saved.

8 This procedure is complete.

Note 1: To return to the Overall GWC upgrade procedure, refer to Overall upgrade process - manual on page 65.

Note 2: To return to the Overall GWC downgrade procedure, refer to Roll back a software upgrade on a GWC node on page 107.

Troubleshooting

The /swd/gwc directory needs to have privileges set to read, write, execute for world access.

At the CS 2000 Core Manager or CBM console

1 Log in to the CS 2000 Core Manager or CBM as the root user.

2 Change directory to the /swd directory by typing

 # cd /swd

and pressing the Enter key.

3 Change the permissions for the gwc directory and its file contents by typing

 # chmod 777 gwc/*

and pressing the Enter key.

4 This procedure is complete.

Firmware flash a GWC card

Purpose of this procedure

Use this procedure to flash the firmware of a GWC card when the version of firmware on the CS 2000 Core Manager or Core and Billing Manager (CBM) is different from the firmware version on one or more GWC cards.

When to use this procedure

Use this procedure when a new GWC firmware load has been delivered on the shelf controller tape (see release notes for the SAM21 shelf controller) and loaded on to the CS 2000 Core Manager or CBM. At this point, the firmware version on the GWC card needs to be upgraded.

Note: This procedure flashes the firmware on the GWC card only if the version of the firmware on the CS 2000 Core Manager or CBM is different from the firmware version on the card. If you need to flash the firmware on a card that contains the same version of the firmware as the CS 2000 Core Manager or CBM, then refer to Force a firmware flash of a GWC card on page 129 in this NTP.

Prerequisites

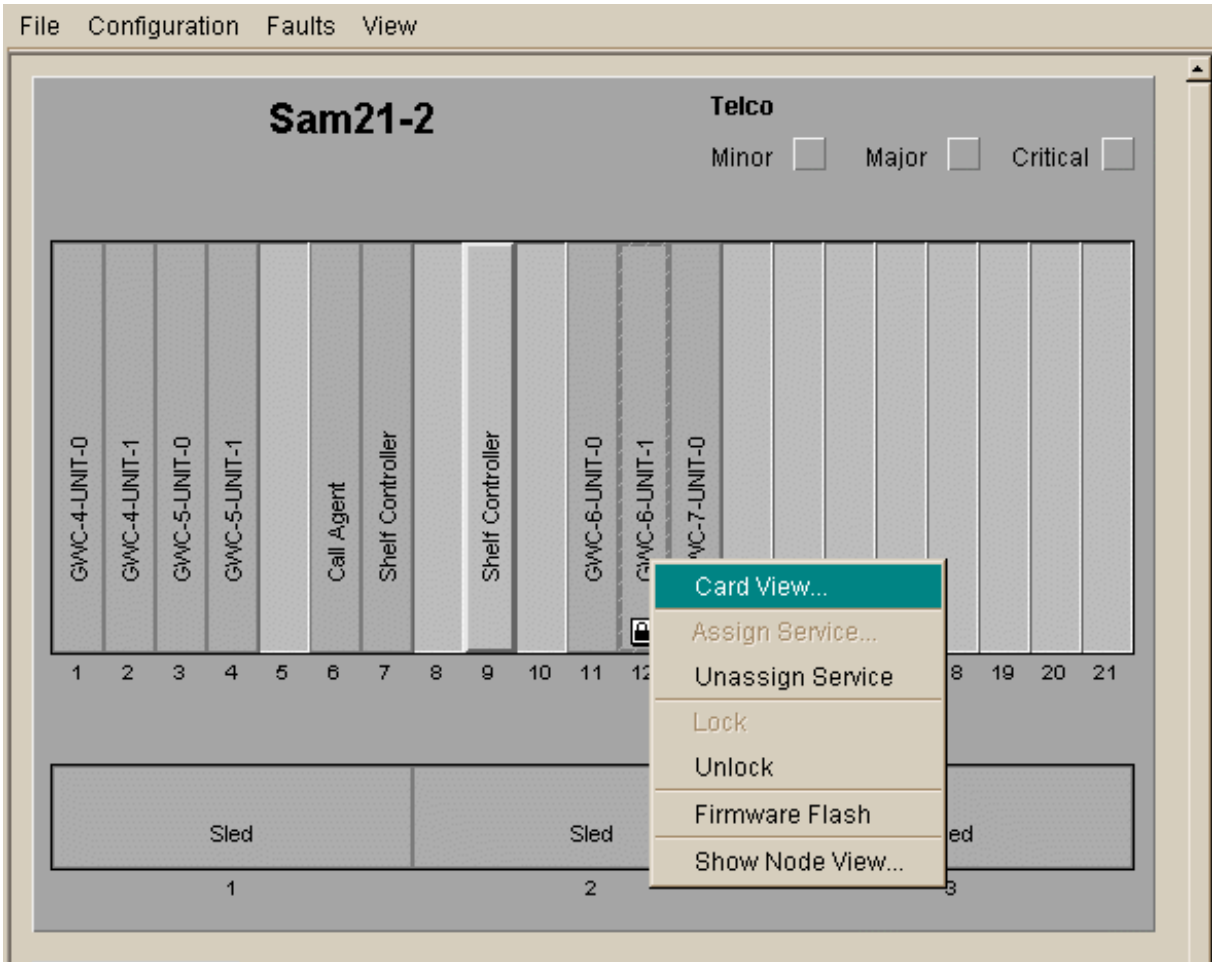
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in *Gateway Controller Security and Administration*, NN10213-611.

Locate the new firmware load for the GWC card that was delivered with the shelf controller software.

Action

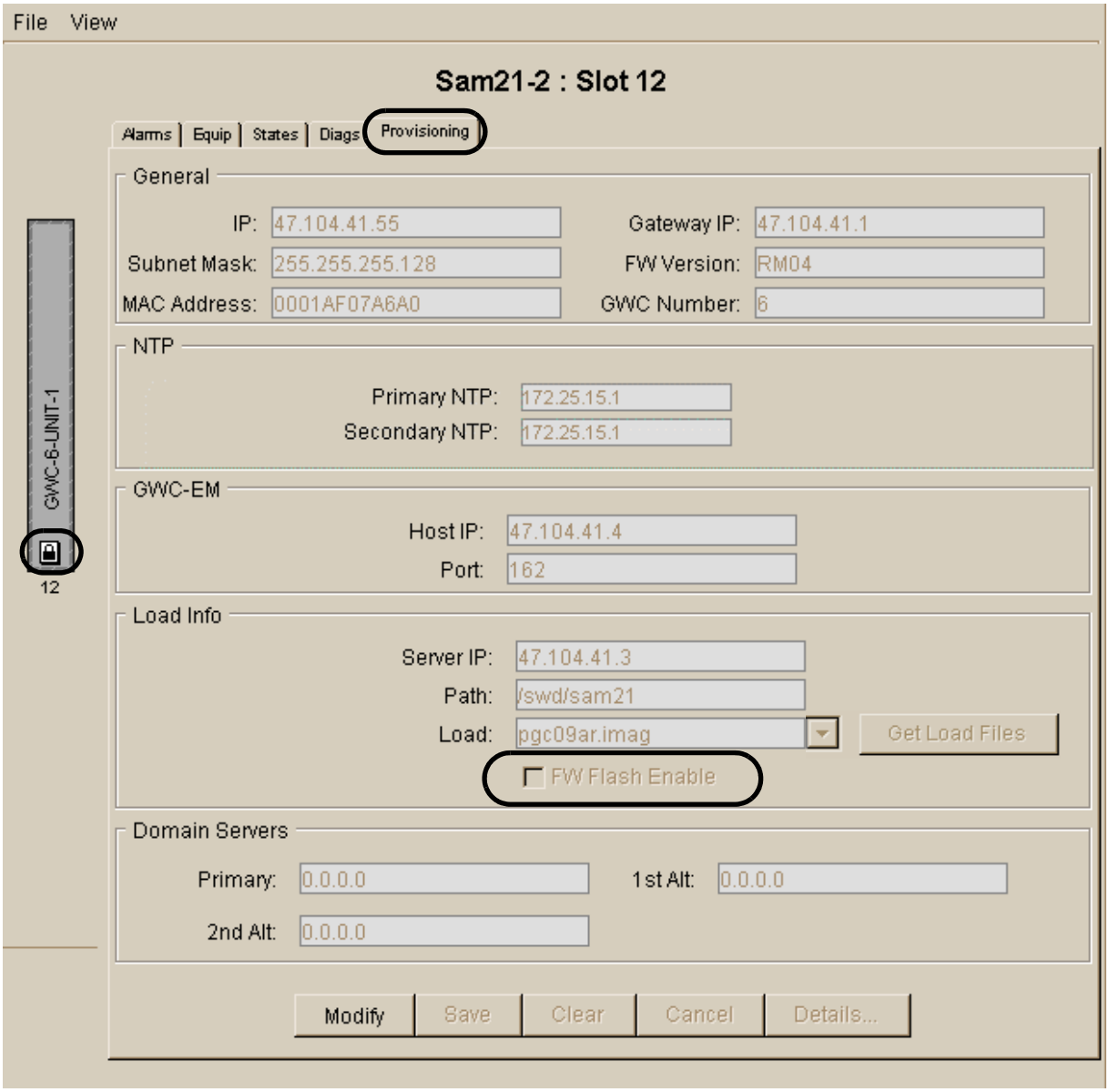
At the CS 2000 SAM21 Manager client

1 From the Shelf View window, right-click on the GWC card scheduled for flashing and select **Card View** from the pop-up menu.



2 Select the **Provisioning** tab in the Card View.

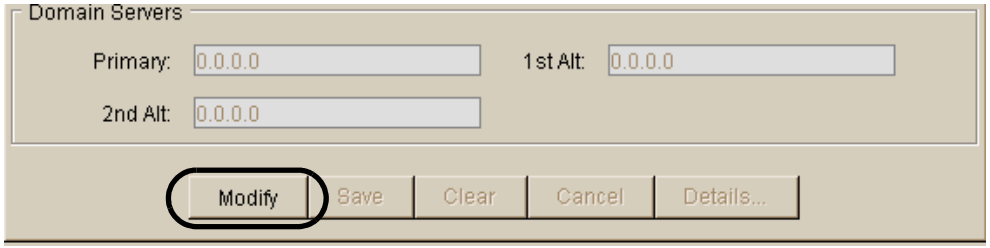
Note: The lock icon should be displayed on the card graphic at the left of the screen. This indicates that the card is locked.



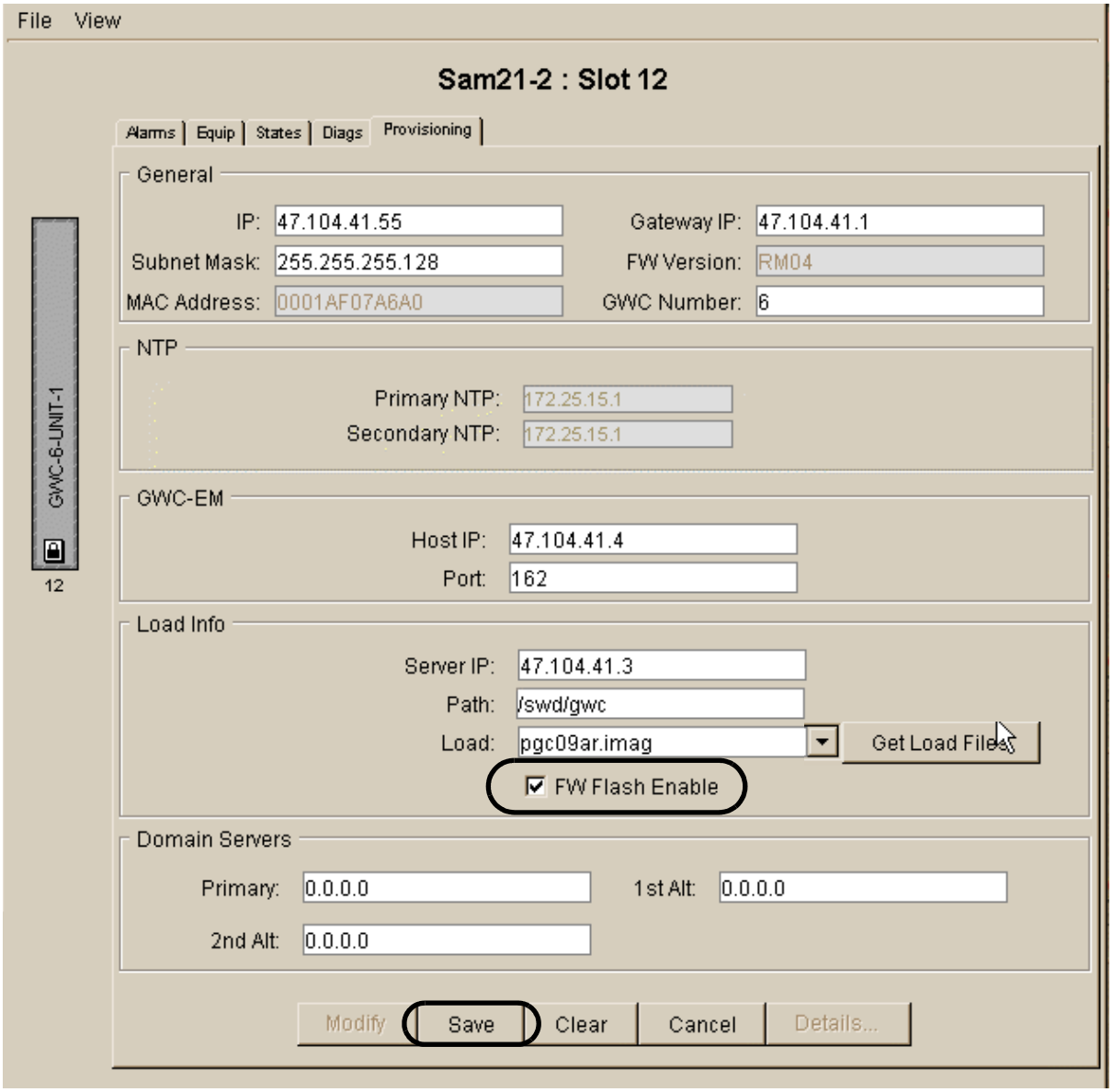
3 If the “FW Flash Enable” checkbox is already selected and a new firmware version is available, the process has already been started. Skip to step 7.

If the **Firmware Flash Enable** checkbox is not selected, continue with step 4.

4 Click the **Modify** button at the bottom of the screen.



5 Select the “FW Flash Enable” checkbox.

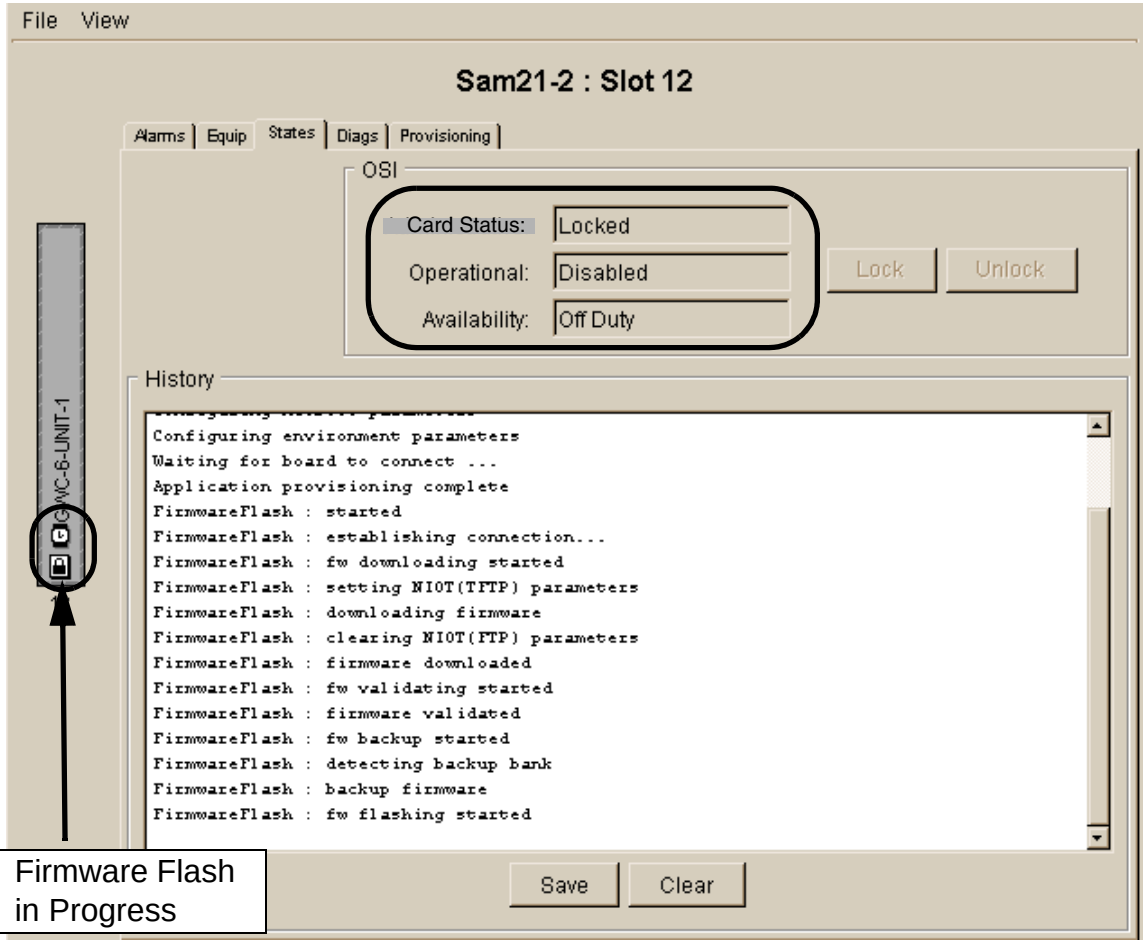


6 Click the **Save** button at the bottom of the screen.

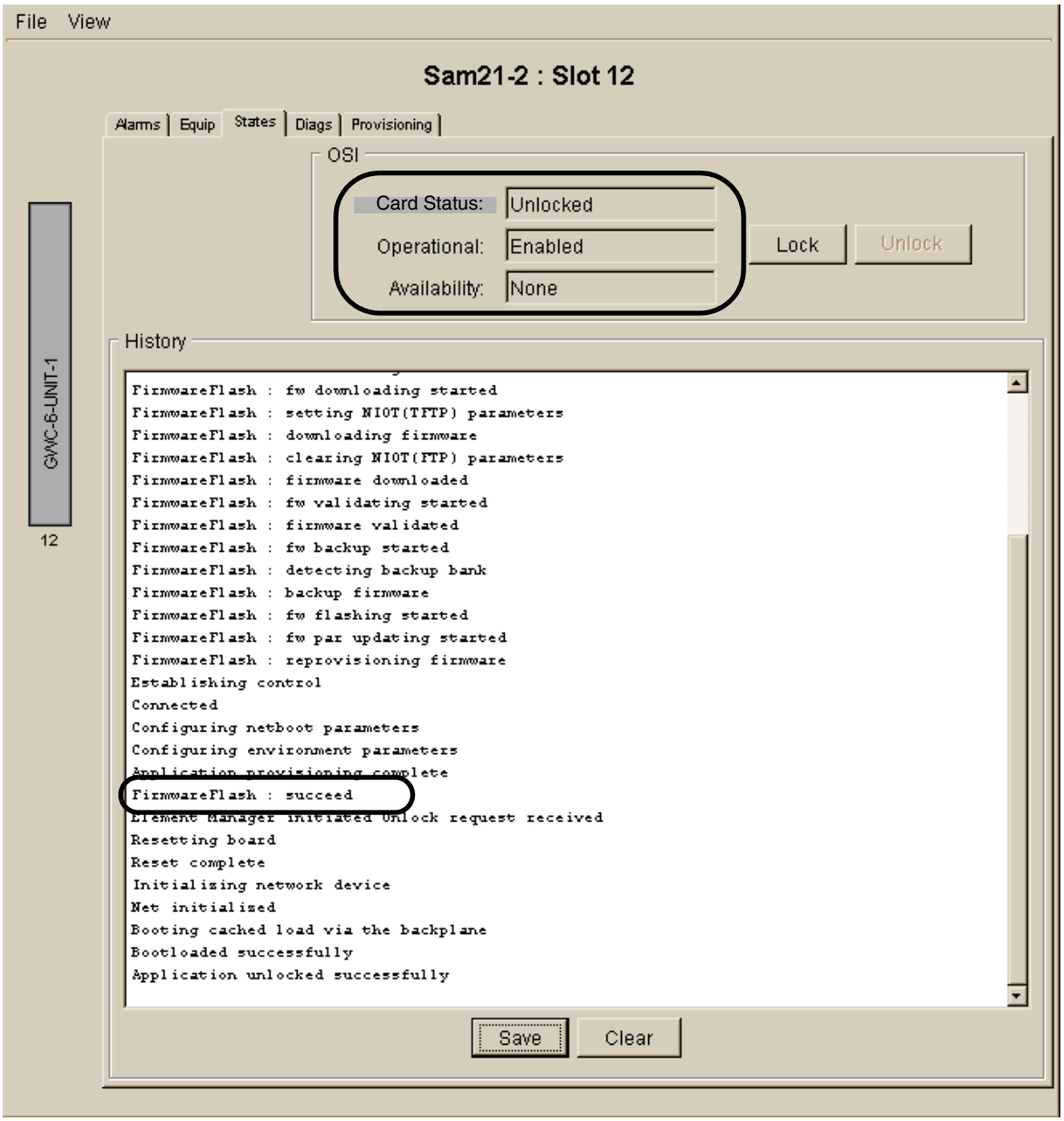
Firmware flashing will begin immediately if a new GWC firmware load is available.

7 Select the **States** tab in the card view.

Observe that the firmware flash icon appears on the GWC card graphic at the left of the screen during the firmware flash. Also observe the card state transition from "locked-disabled-none" to "locked-disabled-off duty". Observe the various firmware flash progress messages in the History window. (Your messages may vary from the graphic below.)



8 The firmware flash icon disappears once firmware flashing is complete. Verify that the firmware flash completed without errors by reviewing the text in the History window. Click the **Unlock** button to unlock the card.



9 Return to step 1 and repeat this procedure for other GWC cards requiring a firmware upgrade.

10 This procedure is complete.

Force a firmware flash of a GWC card

Purpose of this procedure

This procedure forces firmware flashing of a GWC card without any dependency on the firmware version on the card, or the firmware version on the CS 2000 Core Manager or Core and Billing Manager (CBM). This procedure forces firmware flashing of a GWC card even when the CS 2000 Core Manager or CBM and the card have the same firmware version.

Note: If you use the procedure Firmware flash a GWC card on page 123 in this NTP, you will not be able to flash a GWC card's firmware if it has the same firmware version as the CS 2000 Core Manager or CBM.

When to use this procedure

Use this procedure when the firmware on a GWC card is corrupt, or when you suspect a problem with the firmware on a card. This procedure allows you to solve these problems by flashing the same version of the firmware on the CS 2000 Core Manager or CBM.

Prerequisites

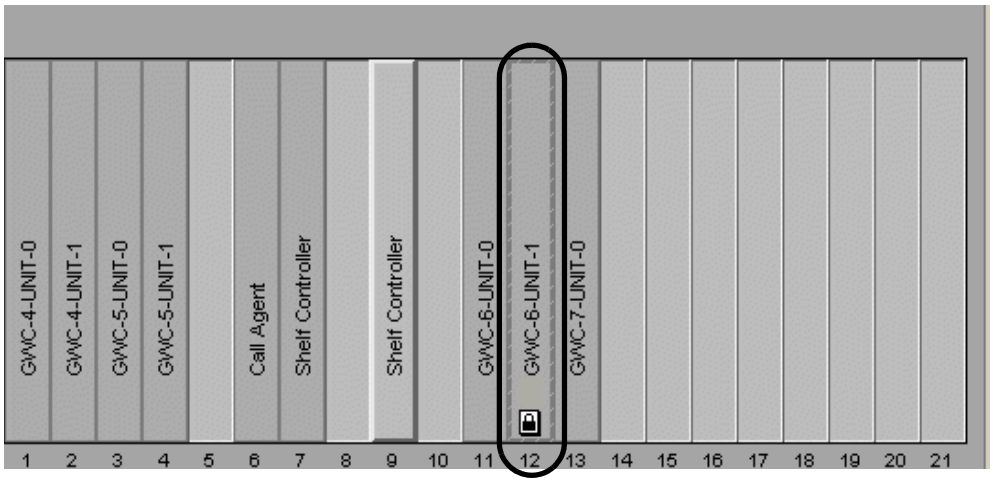
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in *Gateway Controller Security and Administration*, NN10213-611.

Action

At the CS 2000 SAM21 Manager client

1 From the Shelf View window, confirm that the GWC card you want to flash is locked. The lock icon should appear at the bottom of the card.

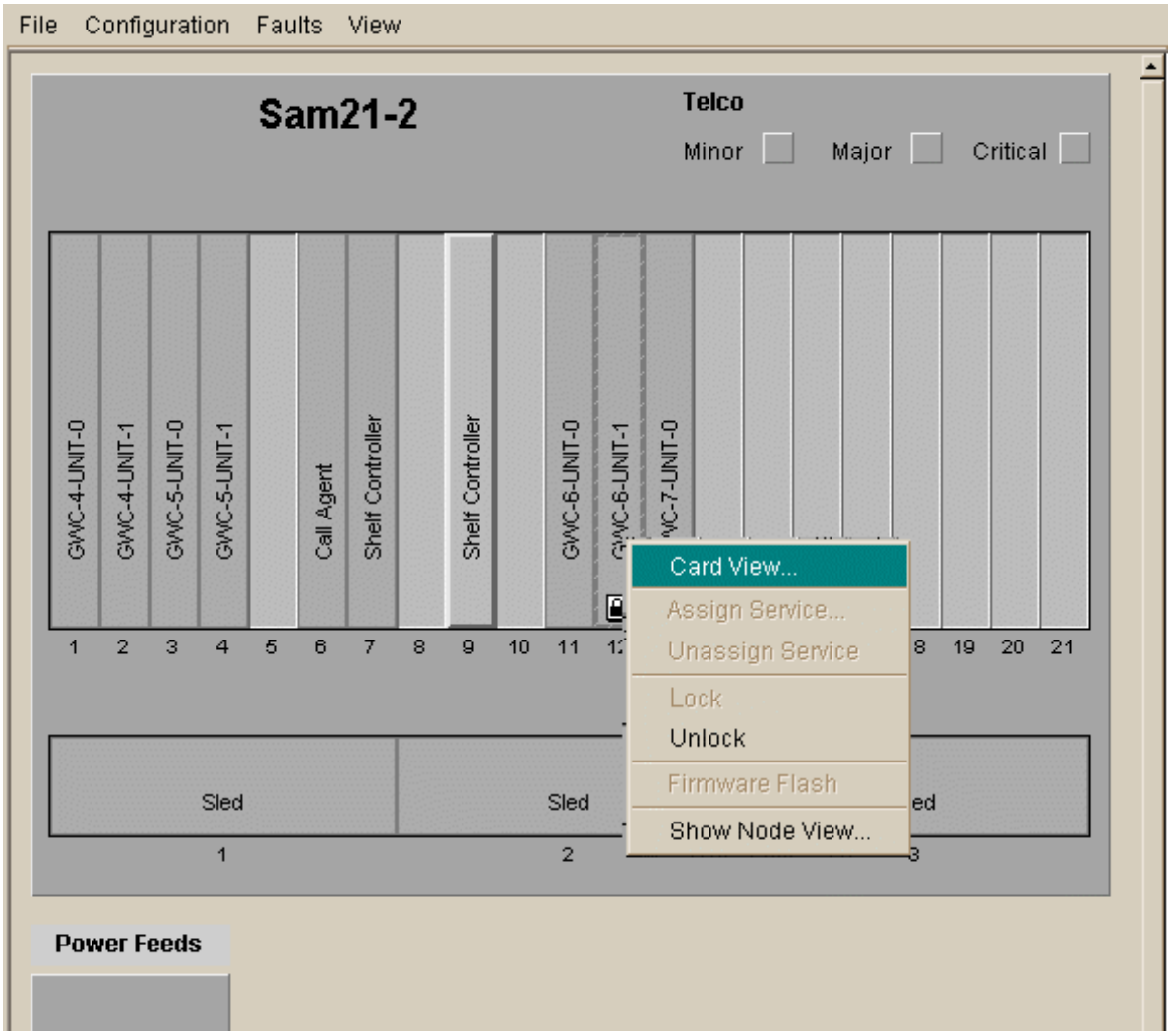
Note: If you have just locked the card using the Card View, click on the **View** menu and select **Shelf View**.



2 From the Shelf View window, right-click on the GWC card scheduled for flashing and determine your next action.

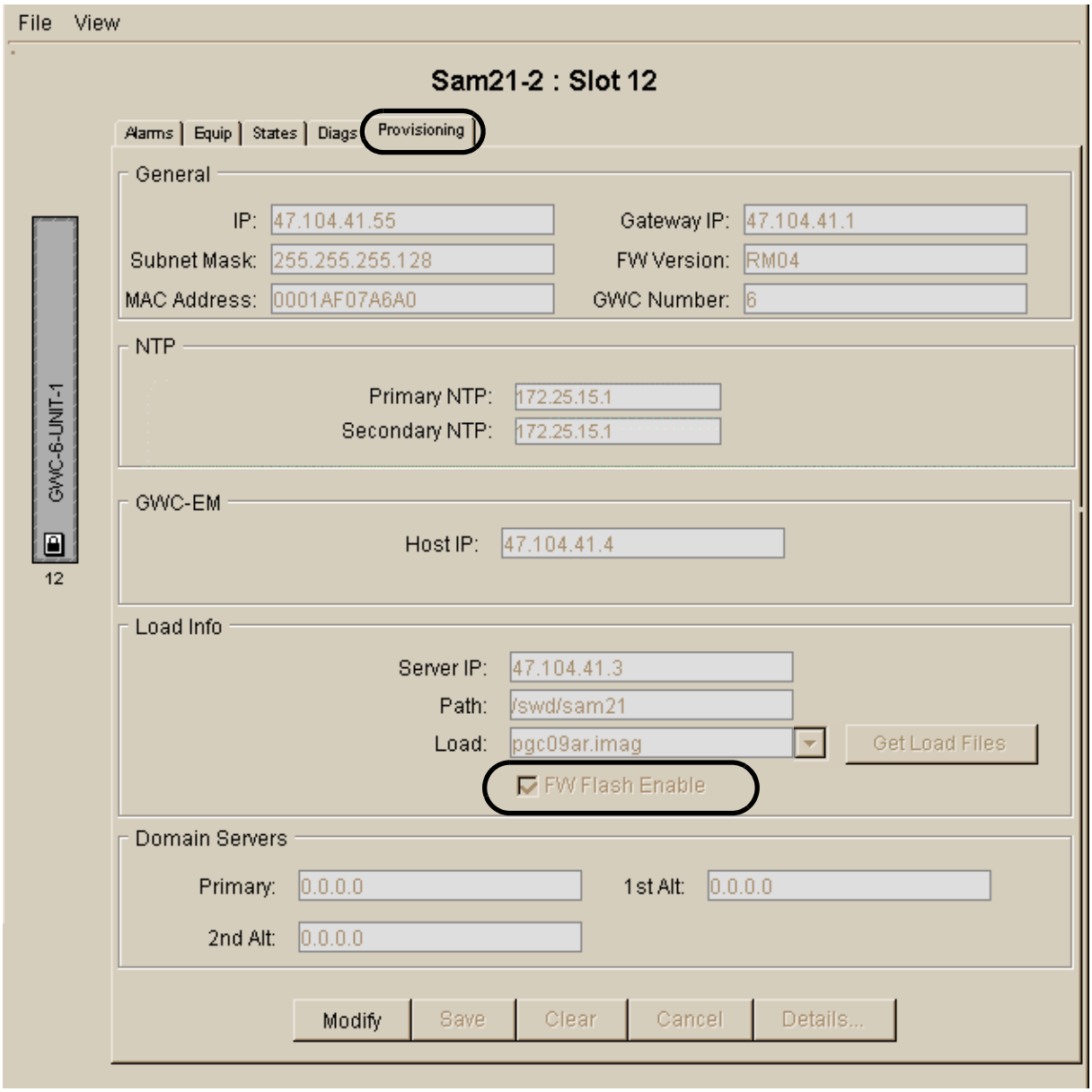
If	Do
If the “Firmware Flash” option is available	skip to step step 8
If the “Firmware Flash” option is not available (the text is faded in the pop-up menu)	go to step 3

3 From the Shelf View window, right-click the GWC card scheduled for flashing and select **Card View**.

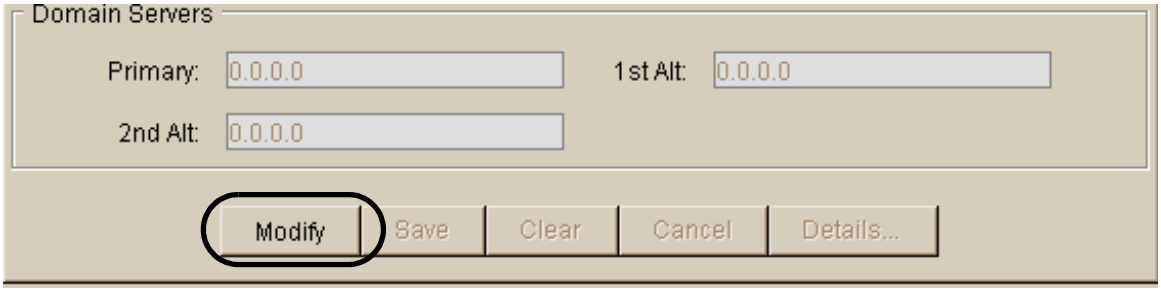


4 In the Card View, select the **Provisioning** tab.

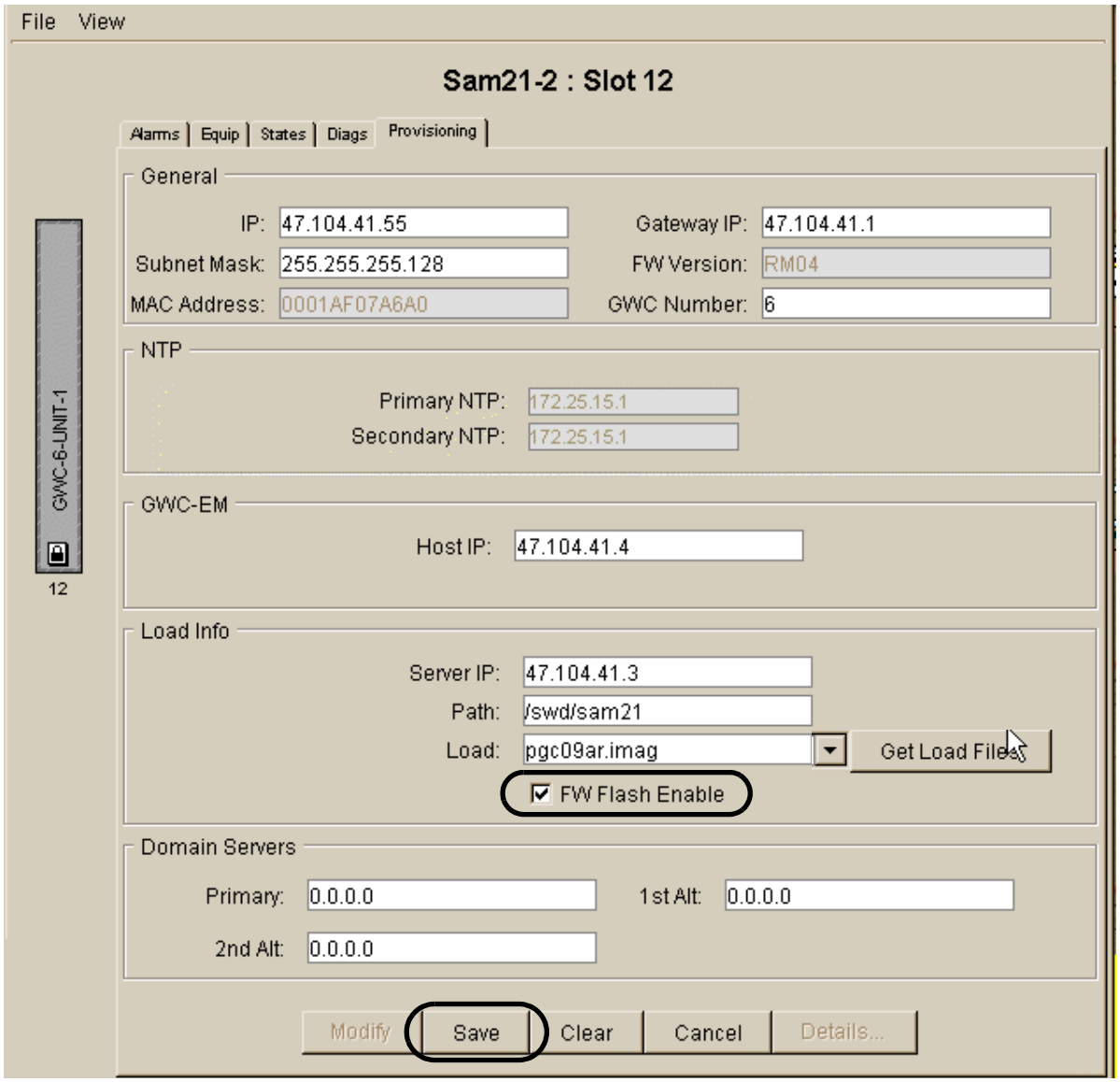
In the Provisioning panel, notice that the **FW Flash Enable** check box is selected. You cannot force a firmware flash if this option is selected.

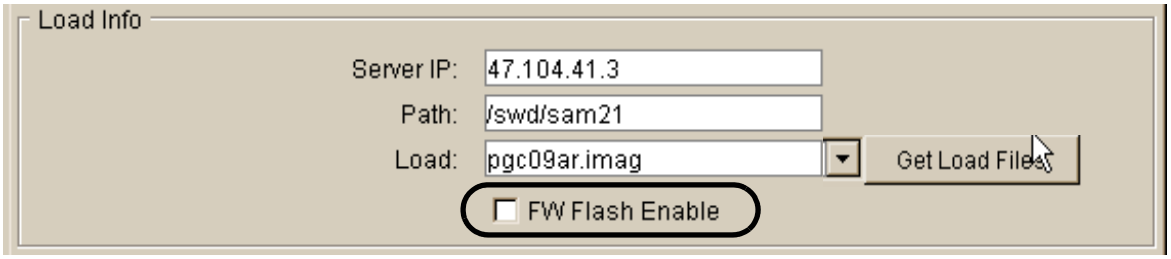


5 In the Provisioning panel, click the **Modify** button.



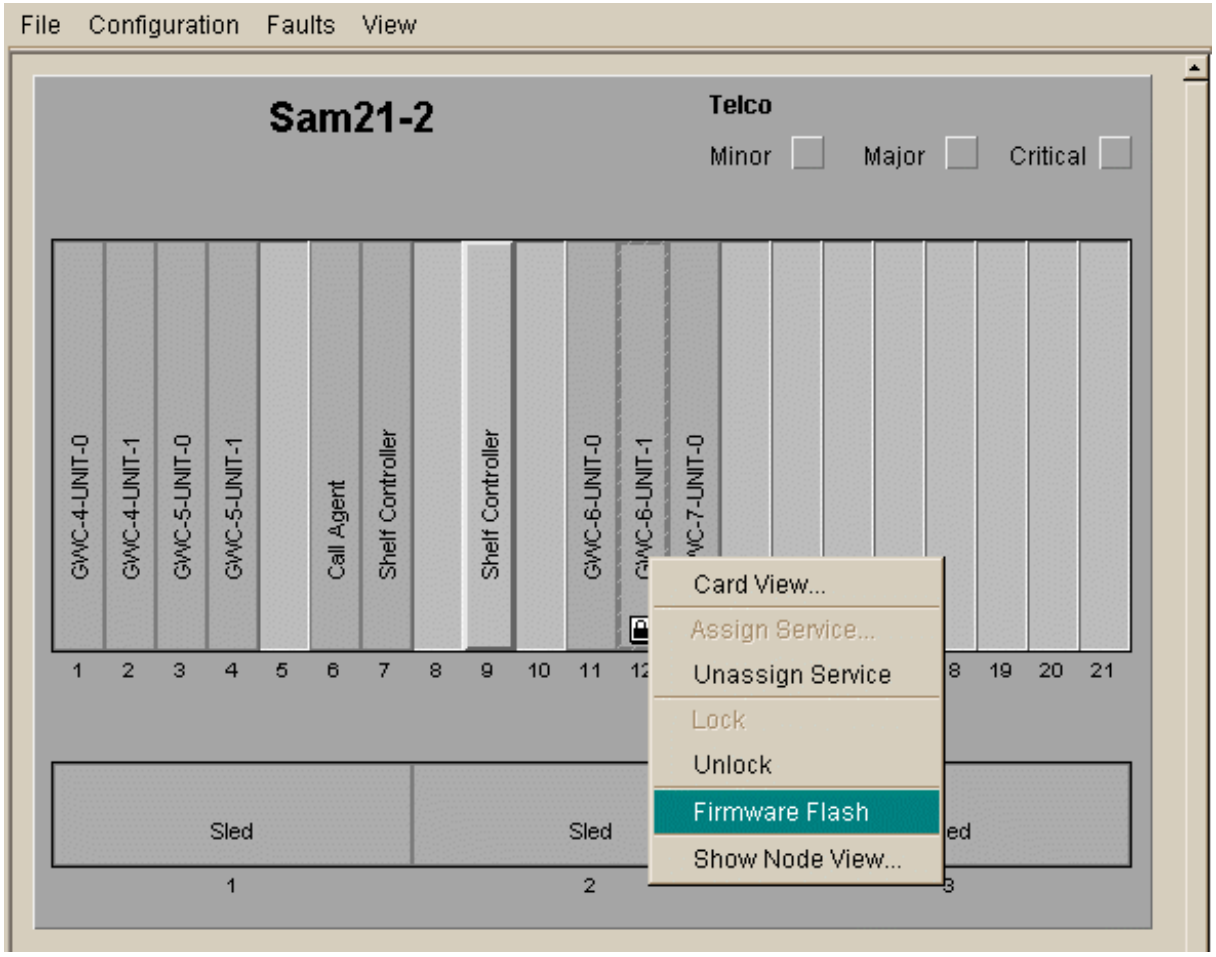
6 In the Provisioning panel, de-select the “FW Flash Enable” check box.





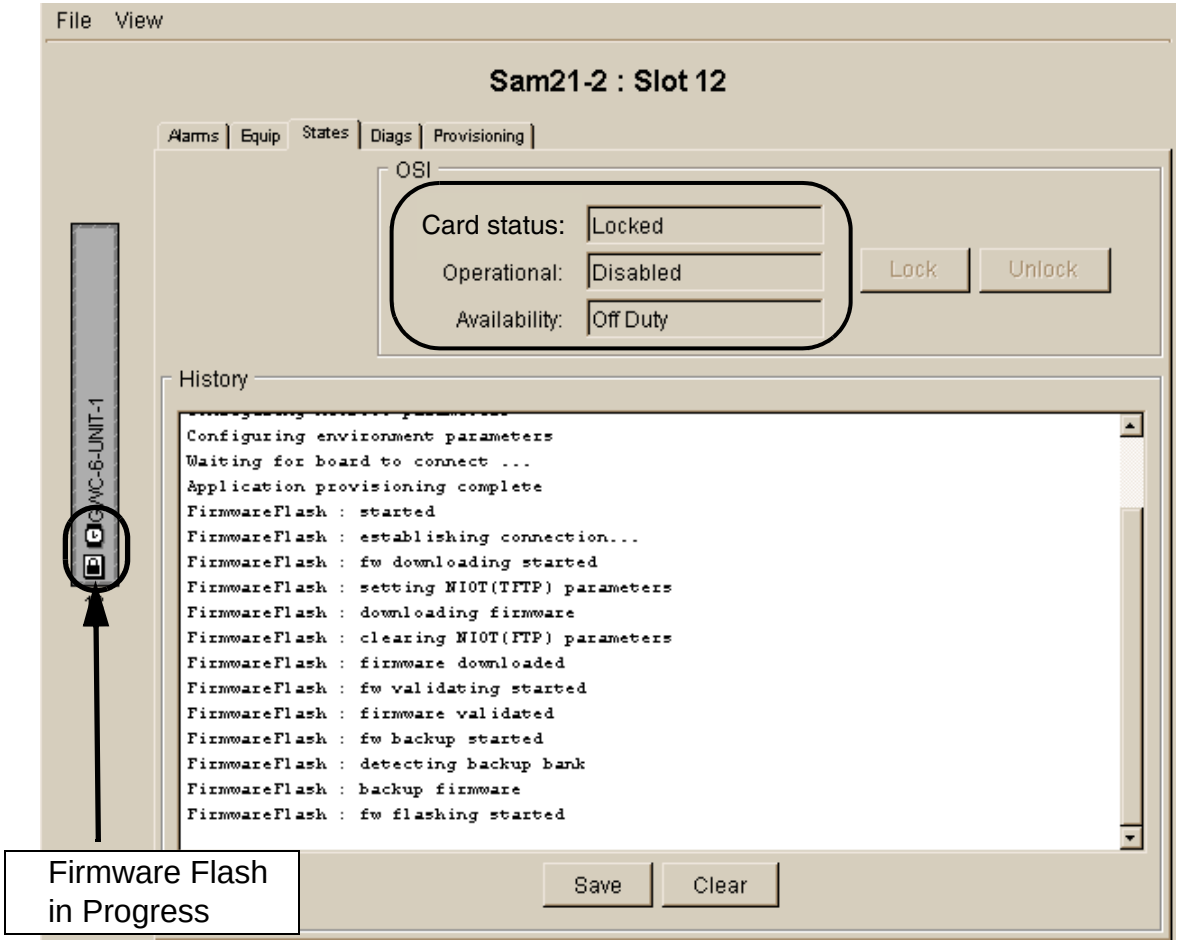
7 Click the **Save** button at the bottom of the screen to save the provisioning change.

8 From the Shelf View window, right-click the GWC card scheduled for flashing and select **Firmware Flash** from the pop-up menu.

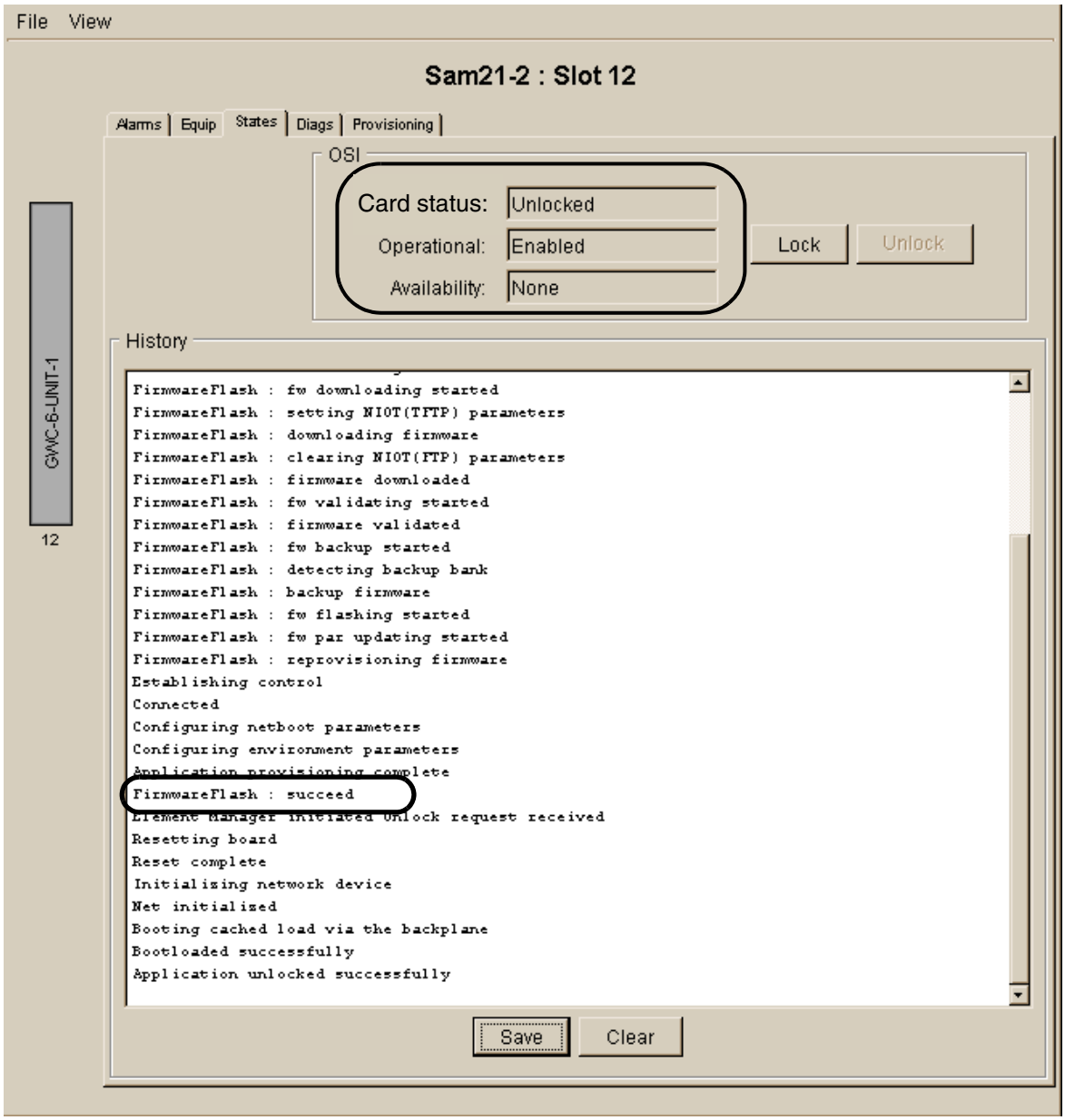


9 Select the **States** tab in the card view.

Observe that the firmware flash icon appears on the GWC card graphic at the left of the screen during the firmware flash. Also observe the card state transition from "locked-disabled-none" to "locked-disabled-off duty". Observe the various firmware flash progress messages in the History window. (Your messages may vary from the graphic below.)



10 The firmware flash icon disappears once firmware flashing is complete. Verify that the firmware flash completed without errors by reviewing the text in the History window. Click the **Unlock** button to unlock the card.



11 Return to step 1 and repeat this procedure for any other GWC cards that require a firmware flash.

12 This procedure is complete.

Enable or disable GWC software auto-imaging

Purpose of this procedure

Use this procedure to enable or disable the auto-imaging of a GWC software load. Auto-imaging provides a mechanism to automatically save up-to-date images of GWC software loads once daily on the CS 2000 Core Manager or Core and Billing Manager (CBM). For more information on GWC software imaging, refer to section GWC software imaging on page 7 in this NTP.

Note: A procedure also exists for taking a manual GWC software image. Refer to Take a manual GWC software image on page 119 in this NTP.

When to use this procedure

Use this procedure when you want to be certain that a new image of a GWC device is saved to the CS 2000 Core Manager or CBM after the device is patched. Auto-imaging is useful in an office where you apply and activate the same patches to all GWCs with the same load.

Note: Auto-imaging is not designed for an office in which different patches are applied to GWCs using the same load.

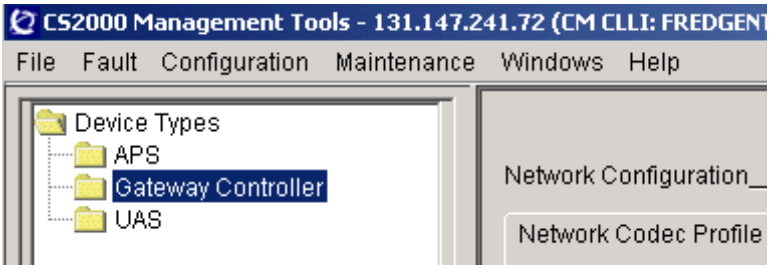
Prerequisites

This procedure has no prerequisites.

Action

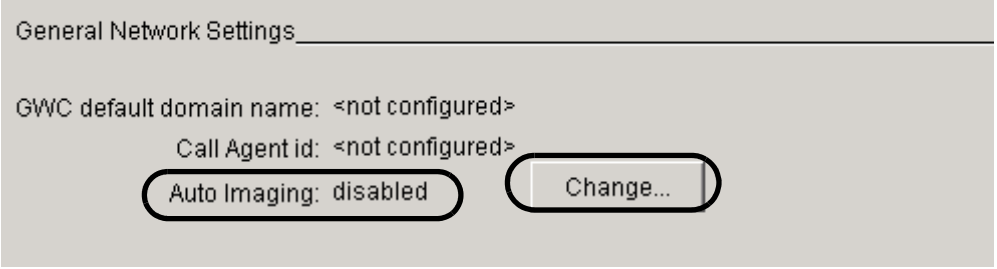
At the CS 2000 GWC Manager client

1 Select Gateway Controller from the Device Types menu.



Look at the current status of Auto Imaging in the General Network Settings area at the bottom of the screen.

The default setting is “disabled”.

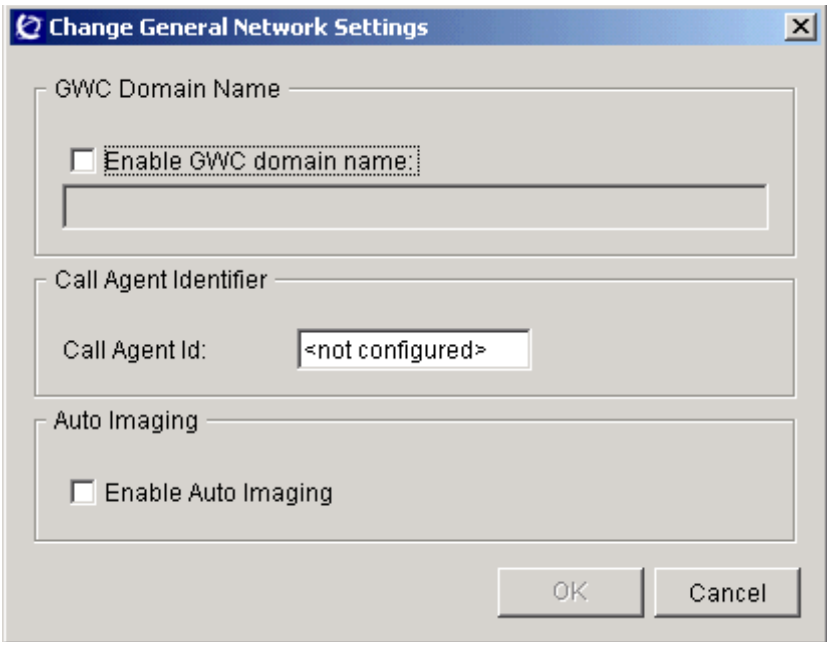


See the following procedures for information on the configuring the other network settings:

- GWC Domain Name - Refer to procedure “Add or change the RMGC default domain” in *Gateway Controller Configuration Management*, NN10205-511.
- Call Agent Identifier (for IP network solutions only, starting in SN07) - Refer to procedure “Set the call agent identifier” in the following locations:
  - *Gateway Controller Configuration Management*, NN10205-511
  - *Upgrading a Carrier Voice over IP Network*, NN10440-450

2 Click the **Change** button to change the status of auto imaging.

The Change General Network Settings dialog box is displayed.



3 Select the Enable Auto Imaging checkbox and click **OK**. An Auto Imaging Enabled message is displayed. Click **OK** to confirm the change.

4 If necessary, you can disable auto-imaging by clicking the **Change** button. At the Change Maintenance Settings dialog box, de-select the “Auto Image Enabled” checkbox and click **OK**. Click **OK** at the message to confirm the change.

5 This procedure is complete.

Troubleshoot GWC upgrades

Purpose of this procedure

This set of procedures is used to troubleshoot failures with GWC upgrades.

When to use these procedures

Use these procedure when:

- the GWC does not RTS
- a warm SwAct has failed
- an image does not load
- you cannot busy an inactive GWC
- callp testing has failed
- imaging of the GWC has failed
- you need to verify a functional BOOTP Service.

Prerequisites

Refer to the individual procedures for any applicable specific prerequisites.

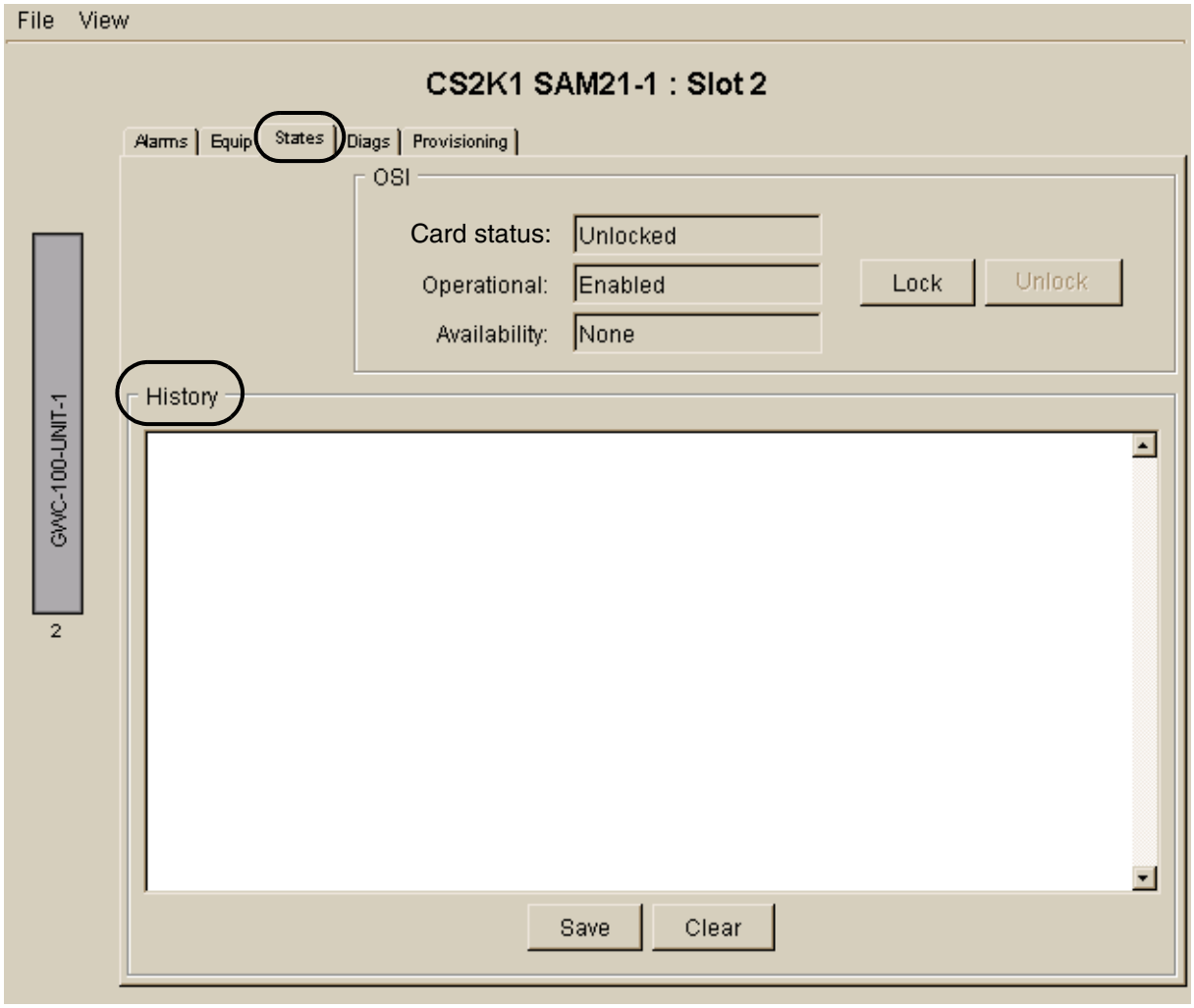
GWC does not RTS

At the CS 2000 SAM21 Manager client

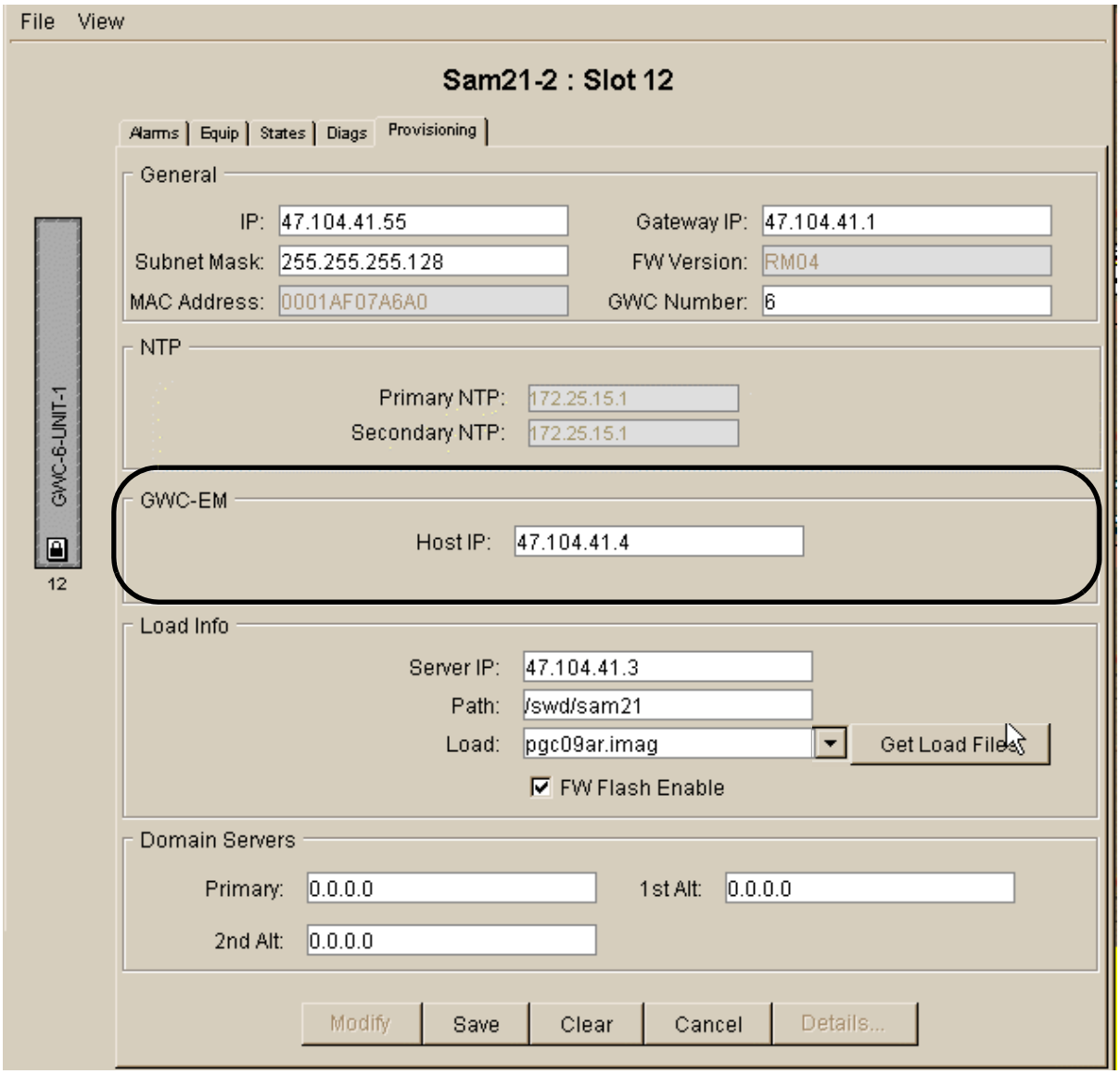
1 If an RTS failure occurs on the inactive GWC unit and the active GWC unit is not “Unlocked” and “Enabled”, then wait for it to become so. If it does not become “Unlocked” and “Enabled”, then lock the active GWC unit from the CS 2000 SAM21 Manager. Locking the Active GWC unit will force a SwAct to the inactive GWC unit.

If the RTS fails after a warm SwAct, go to the troubleshooting procedure Warm SwAct failed on page 144.

2 If the RTS has failed after unlocking the card using CS 2000 SAM21 Manager, review the history log for the unit in the States Pane of the GWC card view. If the history log does not show “Boot image download complete”, then go to troubleshooting procedure Image does not load on page 145.



3 From CS 2000 SAM21 Manager provisioning view, verify that the Host IP address in GWC-EM correctly points to the CS 2000 Management Tools Server. If it is not correct, enter the correct value, then retry locking and unlocking the unit.



4 If you are able to successfully RTS the card, then exit the troubleshooting procedure.

If the GWC does not RTS after 5 minutes, abort further troubleshooting activities and call Nortel for support.

Warm SwAct failed

At the CS 2000 SAM21 Manager client

1 From the CS 2000 SAM21 Manager verify that the inactive unit has properly loaded and RTS'd. If not, retry loading the GWC using troubleshooting procedure GWC does not RTS on page 141.

If the inactive GWC properly loaded and RTS'd, go to the next step.

At the CS 2000 GWC Manager client

2 At the CS 2000 GWC Manger provisioning panel, click the **Warm Swact** button with the **Force** box checked.

If that fails, go to the next step.

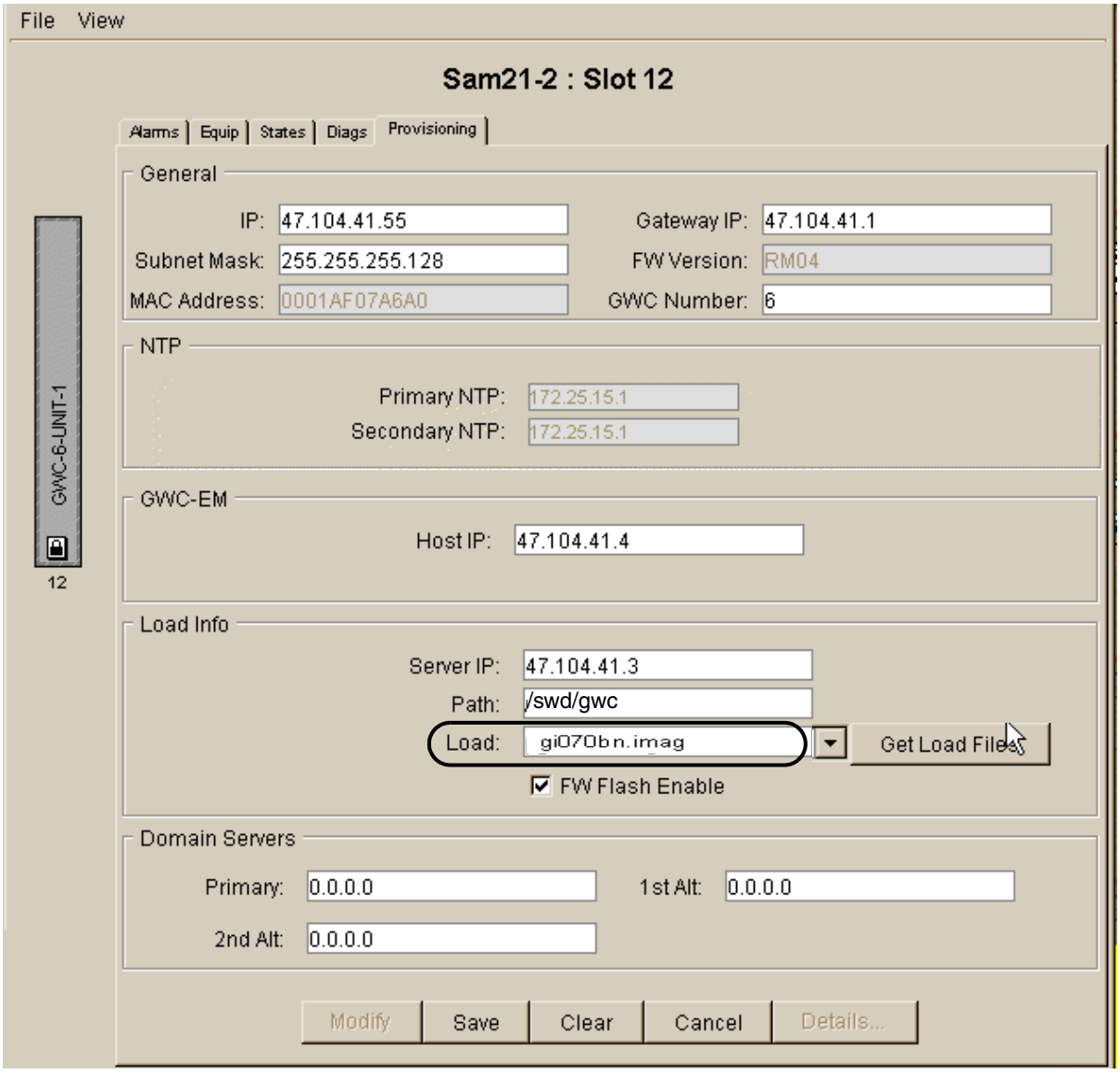
At the CS 2000 SAM21 Manager client

3 At CS 2000 SAM21 Manager, lock the active GWC Unit. This will force a SwAct to the inactive unit.

Image does not load

At the CS 2000 SAM21 Manager client

1 From CS 2000 SAM21 Manager Provisioning Panel, verify that the new load file name matches the file name in the /swd/gwc directory on the CS 2000 Core Manager or Core and Billing Manager (CBM). Also, verify that the file's permissions are set to 755.



2 From the CS 2000 SAM21 Manager Provisioning Panel verify that the file name of the GWC load specified in the “Load” field is correct.

3 Log on to the CS 2000 Core Manger and access the /swd/gwc directory. Verify that the load file size is correct by comparing it with the original source file. If the size is incorrect, then reload the file from its source and set the file permissions to 755.

4 In the CS 2000 SAM21 Manager Provisioning screen verify that the following fields have correct values:

- Load field contains the file name of the new load
- GWC-EM Host IP Address contains the IP Address of the CS 2000 Management Tools Server
- The following fields should contain the original values before the Re-provisioning data was changed to migrate the GWC to the new load and SESM:
  - General/IP - the IP Address of the GWC
  - General/Gateway IP - the IP Address of the default router
  - General/SubNetMask - the subnet mask (e.g. 255.255.255.0)
  - GWC-EM/Port - the TCP/IP port of the GWC-EM trap receiver (162)
  - Load Info/Server IP - the IP Address of the CS 2000 Core Manager or CBM on which the bootp server resides
  - Load Info/Path - The path to the GWC loads (usually /swd/gwc)

5 Verify that the bootp and FTP daemons are running on the CS 2000 Core Manager by referring to the troubleshooting procedure Verifying BOOTP service on page 148.

6 At the CS 2000 SAM21 Manager, retry the “Lock” and “Unlock” operation and see if the unit comes up as “Unlocked” and “Enabled” after approximately 5 minutes. If it does so, exit this procedure with “Success”.

7 If it does not come up, then Call Nortel support and exit this procedure as “Failed”.

Not able to busy inactive GWC

At the CS 2000 GWC Manager client

1 In the CS 2000 GWC Manager Provisioning Panel, determine if the “Usage” state displays as “Busy”. If the state is “Busy” then wait 2 minutes and check again.

2 If it stays busy longer than 2 minutes, then lock the Inactive unit at the CS 2000 SAM21 Manager.

Callp testing fails

At the CS 2000 GWC Manager client

1 At the CS 2000 GWC Manager, verify the codec values in the network configuration settings. If necessary, change them using the procedure “Configure network codec profiles” in *Gateway Controller Configuration Management*, NN10205-511.

2 Retry the Callp test. If it fails again, contact Nortel and abort the upgrade activity.

Imaging of GWC fails

At the CS 2000 Core Manager or CBM console or terminal window

1 If the imaging fails with a Memory Error, abort the Patching Procedure and call Nortel support.

2 If imaging fails with an FTP error, verify that the FTP Server service is running on the CS 2000 Core Manger using the following steps:

- Telnet to the CS 2000 Core Manager or CBM
- Login as root user.
- Type one of the following commands to access the maintenance interface:
  - — **sdmmtc** to access the CS 2000 Core Manager maintenance interface
  - — **cbmmtc** to access the CBM maintenance interface
- Type **mtc** to access the Mtc menu level.
- Type **appl** to display a list of applications and their activity states.

  Locate the application *File Xfer Service* and determine its service status.

If it has the in-service dot (.) under the State column, then the service is up and running. If it displays anything other than a dot (.) such as BSY, OFFL, FAIL, it has a problem.

- Refer to the *Security and Administration* NTP, NN10213-611 (Core and Billing Manager) or NN10358-611 (CBM), for instructions on bringing applications back into service.
- To exit type **quit all.**
- If this procedure fails contact Nortel for support.

Verifying BOOTP service

At the CS 2000 Core Manager or CBM

1 Verify that the BOOTP service is running on the CS 2000 Core Manger or CBM using the following steps:

- Telnet to the CS 2000 Core Manager or CBM
- Login as root user.
- Type one of the following commands to access the maintenance interface:
  - — **sdmmtc** to access the CS 2000 Core Manager maintenance interface
  - — **cbmmtc** to access the CBM maintenance interface
- Type **mtc** to access the Mtc menu level.
- Type **appl** to display a list of applications and their activity states.

  Locate the application *BOOTP Loading Service* and determine its service status.

  If it has the in-service dot (.) under the State column, then the service is up and running. If it displays anything other than a dot (.) such as BSY, OFFL, FAIL, it has a problem.
- Refer to the *Security and Administration* NTP, NN10213-611 (Core and Billing Manager) or NN10358-611 (CBM), for instructions on bringing applications back into service.
- To exit type **quit all.**
- If this procedure fails contact Nortel for support.

Upgrade a GWC node's hardware - MCPN750 to MCPN905

Purpose of this procedure

This procedure describes how to upgrade the hardware of a gateway controller (GWC) node from a pair of MCPN750 cards to a pair of MCPN905 (1 GHz) cards.

Note 1: The new MCPN905 card fits in the same SAM21 frame as the existing MCPN705 card.

Note 2: An MCPN750 GWC pair and an MCPN905 GWC pair can coexist in the same SAM21 shelf.

Note 3: While the MCPN905 upgrade is taking place on the inactive unit of a GWC pair, the active unit (still serviced on the MCPN750 card) is expected to continue to provide service.

Note 4: A mixed configuration (with the active and inactive units serviced by different types of card) is acceptable during the upgrade, but the use of such a configuration for a prolonged period of time is not recommended.

When to use this procedure

This procedure is optional. In SN08, the only call type making use of the MCPN905 card is H.323. Upgrading to the MCPN905 card is recommended if the office uses call type H.323.

If required, use this procedure after fully upgrading the office components (including the GWC) to the latest software release.

Prerequisites

CAUTION

No provisioning activity can occur on the system while the GWC hardware upgrade is in progress.

The prerequisites for this procedure are as follows:

- The GWC must be operating as a duplex node (that is, one MCPN750 running as the active unit, and another MCPN750 as the warm standby unit).
- The upgrade requires two MCPN905 cards.

- The SAM21 EM and SAM21 Shelf Controller must be already upgraded.
- The GWC EM must be already upgraded.

Detailed procedure

At the SAM21 chassis

1 BSY the Inactive unit.

2 Lock the Busy unit.

3 Unprovision the locked unit.

4 Remove the unprovisioned MCPN750 blade.

5 Insert an MCPN905 blade.

6 Provision the blade as a GWC.

Note: The new card must use the same provisioning information (IP address, load file, GWC-EM IP, etc.) as the card it is replacing.

7 Unlock the locked MCPN905.

8 RTS the MCPN905.

9 Verify the MCPN905 transition to InSv (the card should be Inactive and Warm Standby).

10 Warm Swact the GWC node so that the MCPN905 unit is active.

11 BSY the Inactive unit (MCPN750).

12 Lock the BUSY unit.

13 Unprovision the locked unit.

14 Remove the unprovisioned MCPN750 blade.

15 Insert an MCPN905 blade.

Note: The CS 2000 SAM21 Manager displays the new card name (MCPN905) and the corresponding memory size in the Equip tab of the card view.

16 Provision the blade as a GWC.

Note: The new card must use the same provisioning information (IP address, load file, GWC-EM IP, etc.) as the card it is replacing.

17 Unlock the locked MCPN905.

18 RTS the inactive MCPN905.

19 Verify the MCPN905 transition to InSv (the card should be Inactive and Warm Standby).

20 This procedure is complete.