Upgrading the Gateway Controller

What’s new for SN07

The following features or changes affect GWC upgrades for the SN07 release:

- New software load delivery and installation procedure (using CD-ROM).
- New software load delivery and installation procedure (using Electronic Software Delivery)
- New step in the overall upgrade procedure for identifying patches.
- New requirement to set the call agent identifier (ID) for each CS 2000 in your network using the CS 2000 GWC Manager.
- Introduction of the next generation CS 2000 Core Manager: Core and Billing Manager (CBM).
- Restructured the overview section:
  - — Added a new module, Preparing to upgrade the Gateway Controller on page 16.
  - — Moved important pre-upgrade items from the existing overview section to the new module and created a check list for these items.
  - — Removed any overview content that was duplicated in other upgrades documentation.
  - — Updated the overview section to include managing firmware on GWC cards.

- 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	Brand name starting in SN07
Passport Packet Voice Gateway (PVG)	Media Gateway 7400 or 15000
PVG 7400 or PVG 7K	Media Gateway 7400
PVG 15000 or PVG 15K	Media Gateway 15000

Note: The CS 2000 GWC Manager does not reflect these branding changes in SN07. As a result, the GWC customer documentation does not reflect these changes, as well. This table is being 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 NTP thoroughly to learn the different types of upgrades and conditions applied to each upgrade.

The actual GWC software upgrade process is not an automated process, but is instead a set of manual actions you must carry out in a specific sequence on several Carrier VoIP network components.

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

Patches can be applied during an upgrade or on their own as corrective content.

> ***Note:*** Currently, GWC cards are upgraded one at a time. Parallel upgrades of GWC cards is not supported.

Software delivery methods

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

- CD-DROM
- Electronic Software Delivery (ESD)

Delivered load are installed on the CS 2000 Core Manager (SDM) or Core and Billing Manager. Any patch files delivered along with the upgrade load are delivered on CD-ROM and installed on the NPM server. Patches may be included in the load image.

To view any patches that are available with the load image, refer to procedure View the contents of a load file image on page 38. If you want to see what patches are inside the load file, you still must retrieve patch files so that NPM will have the ability to remove the imaged patches.

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

Software patches can also be delivered using electronic software delivery (ESD). For more information on delivering patches, refer to section Patch file acquisition on page 9.

Necessary procedures or checklists used to complete this process are found in “Succession patching” section of the Solution Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

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

For more information about how your site’s ESD is implemented, contact your site network administrator. Also, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP) and the document Electronic Software Delivery Customer Implementation Guide.

Tools and utilities

A GWC software upgrade requires the CS 2000 SAM21 Manager client interface. If GWC software requires patching, the Network Patch Manager (NPM) interface is used to install a patch into GWC software. NPM is an application in the CS 2000 Management Tools suite. This patched load image is optionally saved back to the software load location on the CS 2000 Core Manager or CBM and is available to other GWCs when they reboot. A patched load is saved through the CS 2000 GWC Manager interface. For more information about configuring NPM, refer to the CS 2000 Management Tools section in the ATM/IP Solution-level Configuration Management NTP, NN10409-500. For more information about using NPM, refer to the “Succession patching” section in the Solutions Upgrades NTP, NN10261-450 (for ATM) or NN10344-450 (for IP).

Integrated Element Management System

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

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

- “Launching GWC Manager”
- “Launching SAM21 Manager”

Overall GWC upgrade procedure

The following procedures describe how to upgrade the GWC software and apply patches as part of the same process.

> ***Note:*** Starting in SN07, the call agent identifier (ID) must be set for the CS 2000. This should typically be done prior to upgrading your GWC cards. For details, refer to section “CS 2000 call agent identifier required in SN07” in the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

1. If necessary, complete the following sub-steps using one of the tools available at www.nortelnetworks.com, under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Tools. For instructions on how to use each tool, refer

to the Readme file that can be found under each corresponding link.

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

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

2. If necessary, backup your existing software load file sets using procedure Create a backup of the GWC load file on page 36.

3. Install the new load using one of the following procedures:

   - Deliver and install GWC package using Electronic Software Delivery on page 28

   - Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 23

4. See if any patches are contained within the load image by referring to procedure View the contents of a load file image on page 38.

5. Upgrade software on a seed GWC unit that is inactive using procedure Upgrade a standby GWC card software load on page 42.

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

7. Patch the same seed GWC unit using the following procedures:

   a. Audit the GWC unit for necessary patch activity using procedure Perform a device audit using the NPM on page 84.

   b. Transfer patches to the Network Patch Manager (NPM) database using procedure Transfer patches to the NPM database manually on page 89.

   c. You may also define reports for a GWC using procedure Define reports using the NPM on page 94.

   d. Apply patches using procedure Apply patches using the NPM on page 101.

   e. Activate patches using procedure Activate patches using the NPM on page 110.

   f. Deactivate any obsolete patches using procedure Deactivate patches using the NPM on page 121.

   g. Remove any obsolete patches using procedure Remove patches using the NPM on page 132.

8. Complete procedure Take a manual GWC software image on page 141.

9. Perform a warm SwAct on the GWC units in the node.
   Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for a procedure to perform a warm SwAct.

   Note: Instructions for steps 9, 10 and 11 in this procedure are also available within the procedure Upgrade a standby GWC card software load on page 42 in this NTP.

10. Perform the following steps on the new standby GWC unit.
    Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform each of the following tasks.

    a. Busy the new standby unit.

    b. Lock the new standby unit.

    c. Update the new standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 42.

    d. Unlock the new standby unit.

11. Access the next GWC node and perform the following steps.
    Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to perform each of the following tasks.

    a. Busy the standby unit.

    b. Lock the standby unit.

    c. Update the standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 42.

    d. Unlock the standby unit.

    e. SwAct the GWC units in the node.

    f. Busy the new standby unit.

    g. Lock the new standby unit.

h. Update the new standby unit with the patched GWC load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Upgrade a standby GWC card software load on page 42

i. Unlock the new standby unit.

12. Repeat step 11 for each GWC node until all units in each node are rebooted from the new image.

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

Overall GWC downgrade procedure

The reversion or downgrade procedures describe how to roll back a software upgrade and how to remove patch files.

Note 1: If your system contains shared network address translators (NATs) that have been manually assigned a middlebox ID, you must delete all instances of these NATs before downgrading to a software load earlier than SN07. Refer to procedure “Delete a NAT device” in the Gateway Controller Configuration Management NTP, NN10205-511.

Note 2: If you suspect that the call agent ID for your CS 2000 has ever been changed, contact Nortel customer support before attempting to roll back to a software load earlier than SN07.

1. Rollback the software load on the standby GWC in a node using procedure Rollback a software upgrade on a standby GWC on page 57.

2. If necessary, patch the earlier software load on a seed GWC unit using the following procedures:

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

   a. Audit the GWC unit for necessary patch activity using procedure Perform a device audit using the NPM on page 84.

   b. You may also define reports for a GWC using procedure Define reports using the NPM on page 94.

   c. Apply patches using procedure Apply patches using the NPM on page 101.

   d. Activate patches using procedure Activate patches using the NPM on page 110.

   e. Deactivate any obsolete patches using procedure Deactivate patches using the NPM on page 121.

   f. Remove any obsolete patches using procedure Remove patches using the NPM on page 132.

3. Complete procedure Take a manual GWC software image on page 141

4. Perform a warm SwAct on the GWC units in the node.
   Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for a procedure to perform a warm SwAct.

   Note: Instructions for steps 4, 5 and 6 in this procedure are also available within the procedure Rollback a software upgrade on a standby GWC on page 57 in this NTP.

5. Perform the following steps on the new standby GWC unit.
   Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to busy, lock and unlock a GWC unit.

   a. Busy the new standby unit.

   b. Lock the new standby unit.

   c. Update the new standby unit with the earlier GWC software load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Rollback a software upgrade on a standby GWC on page 57.

   d. Unlock the new standby unit.

6. Access the next GWC node and perform the following steps.
   Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for procedures to busy, lock, unlock and SwAct GWC units.

   a. Busy the standby unit.

   b. Lock the standby unit.

   c. Update the standby unit with the earlier GWC software load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Rollback a software upgrade on a standby GWC on page 57.

   d. Unlock the standby unit.

   e. SwAct the GWC units in the node.

   f. Busy the new standby unit.

g. Lock the new standby unit.

h. Update the new standby unit with the earlier GWC software load using the CS 2000 SAM21 Manager. Refer to the appropriate steps in the procedure Rollback a software upgrade on a standby GWC on page 57.

i. Unlock the new standby unit.

7. Repeat step 6 for each GWC node until all units in each node are rebooted from the new image.

Troubleshooting upgrade problems

Should any problems occur during upgrade, or rollback (downgrade) activities, refer to procedure Troubleshoot GWC upgrades on page 162 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 “Succession patching” section in the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

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

Patch file acquisition

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

- Drop box - patch files are pushed from Nortel Networks to an external drop box location. The drop box can exist on Nortel

Networks' Customer Access Network (CAN), or the customer's wide area network (WAN).

- Web distribution - patches are pulled through the Internet from a secure Nortel Networks web page and stored on a customer-provided server. Web distribution is done through www.nortelnetworks.com. Patches are located under Support -> Software Downloads -> Succession -> Succession Communication Server 2000 -> Software.

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

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

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

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

Patch activation

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

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

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 will replace 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 only be replaced 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 will remain 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 the ATM/IP Solution-level Security and Administration NTP, 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 will 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 141
- 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 159

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

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

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 NTP.
- 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 145.
- To resolve problems with the firmware on a GWC card, refer to procedure Force a firmware flash of a GWC card on page 151.

Preparing to upgrade the Gateway Controller

This section provides details on specific items that personnel need to be aware of prior to upgrading GWC nodes in a CS 2000.

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

GWC upgrade preparation list

Item	√	Details
Upgrade paths supported		Depends on your solution. See the supported upgrade paths in your solution's upgrade NTP, NN10344-450 or NN10261-450.
Upgrade order for all GWC card types		Applicable to all solutions. See section Upgrade order for all GWC card types on page 17.
Upgrade and downgrade call service impact		Applicable to all solutions. See Upgrade and downgrade call service impact on page 19.
PVG trunk GWC upgrades and downgrades		Applicable to IP and AAL2 solutions. See PVG trunk GWC upgrades and downgrades on page 20.
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 21.
Allocate time for a GWC upgrade		Applicable to all solutions. See Allocating time for a GWC upgrade on page 22.
Impact of an upgrade on GWC configuration		Applicable to all solutions. See Impact of an upgrade on GWC configuration on page 22.

Upgrade order for all GWC card types

All GWC cards of the same type must be upgraded before moving on to the next group. For example, all audio controller GWC cards must be upgraded before upgrading the next GWC card-type present in your system.

The order presented includes all GWC card types, even though some of the card types indicated cannot co-exist in the same installation. For the GWC card type order specific to your solution, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

Upgrade GWC card pairs from SN05, SN06, SN06.2, or SN07 to SN07 in the following order of card type:

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

GWC card type upgrade order

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

Note 1: The Session Server (SS) is a new component in SN07. It can replace the Virtual Routing Destination Node (VRDN) GWC as a SIP-T interface. The following office configurations are supported in SN07: SS only, VRDN SIP-T only, or VRDN SIP-T and SS co-existing in the same office. For the upgrade order specific to your solution, refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP).

Note 2: Offices can only have one GWC with an RA. Therefore, an office will either have a SIP-T/APG/RA GWC or an APG/RA GWC but not both. In addition, some non-AAL1 solutions will support provisioning a combination of DPT and APG endpoints on the same GWC. This allows endpoints of different GWC types to coexist on the same GWC card. Referred to as a “combo profile”, the GWC is limited to 1008 APG ports, while the APG standalone is limited to 3024 APG ports. The RA server can be included or excluded on the same GWC under both APG capacity variants.

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

Note 4: Starting in SN06, the Redirecting media gateway controller (RMGC) application migrates from the CS 2000 Management Tools server to the GWC platform. RMGC service cannot be provided between upgrading the CS 2000 Management Tools server and commissioning the GWC-based RMGC service. Refer to the Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP) for a complete migration strategy for this feature.

It is assumed that an existing Audio Controller GWC will be used to host the RMGC application. If commissioning a new GWC for RMGC in SN07, refer to appropriate procedures in the Gateway Controller Configuration Management NTP, NN10205-511.

Upgrade and downgrade call service impact

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

> ***Note:*** Contact Nortel customer support for information on call service impact regarding any upgrade involving SN06.1.

Upgrade and downgrade call service impact

GWC type	SN05/06/6.2 -> SN07 Upgrade	SN07 -> SN07 Maintenance (Patching)	SN07 -> SN06.2/06 Downgrade	SN07 -> SN05 Downgrade
AUDCNTL	Stable announcement and conference calls survive.	Stable announcement and conference calls survive.	Stable announcement and conference calls survive.	Stable announcement and conference calls not using SN07 features survive.
VRDN	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	ALL calls survive.	Calls not using SN07 features survive.
SIP-T	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	NO calls survive.	NO calls survive.
PVG Trunk	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	NO calls survive.	NO calls survive.
APG	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	SIP-T calls using an APG do not survive.	SIP-T calls using an APG do not survive.
Line or H.323	Stable 2-party calls survive. Possible limited functionality after the swact. 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. Billing records might not be produced when calls go on-hook. H.323 gateway-based calls will not survive.	SOME calls may survive. Billing records might not be produced when calls go on-hook. H.323 gateway-based calls will not survive.

PVG trunk GWC upgrades and downgrades

SN05 to SN07 upgrades and SN07 to SN05 downgrades to PVG TDM trunk GWCs are impacted by changes in the IP IW SPM and the CS 2000 software loads. This item applies to IP and AAL2 solutions. These changes involve how echo cancellation (ECAN) is managed to accommodate the IP IW SPM. In an SN05 to SN07 upgrade, the GWC is upgraded before the CS 2000. Once the PVG GWC is upgraded to software release GC07/GT07, it will manage ECAN control for PVGs differently. This change also has an impact on upgrade rollbacks. The details of this change are as follows.

Prior to SN06, if a trunk GWC-based ISUP or PRI trunk group was datafilled in table TRKSGRP with field ECSTAT set to EXTERNAL, the GWC would send a command to activate the echo canceller integrated in the TDM gateway for that trunk group. This would occur unless ISUP or PRI messaging indicated that echo cancellation was already being performed between the echo cancellation and the source of the echo. If the ECSTAT field was not set to EXTERNAL for an ISUP or PRI trunk (that is, it was set to NONE), the echo canceller in the gateway would not be activated by the GWC under any circumstances.

In SN06 and any subsequent releases, this behavior is essentially reversed such that the echo canceller in the gateway will be activated automatically if the ECSTAT field is set to INTERNAL on GWC-based ISUP or PRI trunk types. If the ECSTAT field is set to EXTERNAL, it is assumed that an external echo canceller exists on the TDM trunk connected to the TDM gateway and that the external echo canceller has cancelled the echo. Therefore, if the TRKSGRP ECSTAT field is set to EXTERNAL, the echo canceller in the gateway will not be activated.

The new interpretation of the ECSTAT field will take effect upon activation of the GC07/GT07 GWC software load, after the upgraded trunk GWC card is rebooted. The only valid values for TRKSGRP field ECSTAT for GWC PRI and ISUP trunks in SN07 will be EXTERNAL or INTERNAL.

On upgrade from SN05 to SN07, GWC ISUP trunks datafilled as EXTERNAL will be reformatted to INTERNAL. GWC PRI trunks will be reformatted to INTERNAL. GWC ISUP and PRI trunks will always indicate to upstream or downstream switches that echo cancellation has been applied on the TDM interface (either externally or internally). During a GWC upgrade from SN05 to SN07, the following occurs:

- When the inactive side of the GWC is loaded with the GC07/GT07 load or later, the trunk sub group data in the GWC will change

ECSTAT from NONE to EXTERNAL and from EXTERNAL to INTERNAL.

- When the Core is upgraded to SN07, the same table changes will occur for GWC based trunk groups only.

If a GWC is rolled back (downgraded) from SN07 to SN05, then all the trunks on that GWC have to be BSY/RTS so that they receive the right ECSTAT datafill. However, the rollback must occur before the Core is upgraded for the BSY/RTS of the GWC to have the correct effect. If the Core is already upgraded and rolled back, the TRKSGRP data is not reverted and a subsequent rollback of the GWC to SN05 will result in incorrect ECAN behavior on all GWC based ISUP and PRI trunk groups.

Ensuring compliant characters in RMGC application domain name

If you are upgrading to SN07 and intend to use the Redirecting Media Gateway Controller (RMGC) application, you need to be aware that using invalid or non-RFC 1034 compliant characters (such as the underscore character) for the GWC domain name in the GWC database could render the RMGC application unusable. Check the cmshortCLLIname in the XA-Core table OFCENG before the upgrade begins to determine if it uses any characters that are not compliant with RFC 1034. Correct this value before the upgrades are started on the XA-Core. Refer to your applicable Office Parameter Reference Manual, NTP 297-8001-855 or NTP 297-9051-855, to perform this task.

Consult your site system administrator for assistance in determining the domain name for your site. If you are commissioning a new GWC for RMGC in SN07, refer to procedures in the GWC Configuration Management NTP, NN10205-511.

Allocating time for a GWC upgrade

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

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

- Total upgrade time for each GWC pair is 24 minutes (12 minutes for each card)
- Time needed to apply GWC fileset to CS 2000 Core Manager or CBM is 5 minutes
- Time to perform a GWC node warm SWACT is 1 minute
- Time to post upgrade call processing check for each GWC node is 2 minutes

Impact of an upgrade on GWC configuration

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

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

Purpose of this procedure

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

> ***Note:*** For information on how to deliver and install GWC load using the Electronic Software Delivery (ESD) method, refer to procedure Deliver and install GWC package using Electronic Software Delivery on page 28

When to use this procedure

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

Prerequisites

This procedure has no prerequisites.

Action

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

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

At the CS 2000 Management Tools terminal

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

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

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

3 Execute the installation script by typing

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

and pressing the Enter key.

Example response:

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

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

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

 Please choose one of the following: 1
```

4 Install the software by typing

> 1

and pressing the Enter key.

The system displays the contents of the .rpm package.

Example response:

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

/swd/gwc/gn070be.imag

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

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

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

> Y

and pressing the Enter key.

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

Example response:

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

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

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

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

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

Example response:

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

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


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

7 Exit the installation program by typing

```
# x
```

and pressing the Enter key.

8 Use the following table to determine your next step.

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

At the CS 2000 Core Manager console or terminal window

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

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

10 Access the gwc directory by typing

```
# cd /swd/gwc
```

and pressing the Enter key.

11 Execute the GwcConfig.sh script by typing

```
# ./GwcConfig.sh
```

and pressing the Enter key.

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

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

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

14 Log out of the CS 2000 Core Manager by typing

```
# exit
```

and pressing the Enter key.

At the CS 2000 Management Tools terminal

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

```
# eject cdrom
```

and pressing the Enter key.

16 Log out of the CS 2000 Management Tools server.

17 This procedure is complete.

Deliver and install GWC package using Electronic Software Delivery

Purpose of this procedure

This procedure describes how to transfer Gateway Controller (GWC) software loads from Nortel Networks to a customer drop box using the Electronic Software Delivery (ESD) method, and how to install the transferred load onto the CS 2000 Core Manager or Core and Billing Manager (CBM).

> ***Note:*** For information on how to install GWC load from CD-ROM, refer to procedure Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 23.

When to use this procedure

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

- GWCC0070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard NCL release
- GWCW0070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for standard International NCL release
- GWC0M070.n.V.NCL.NAP.VAULT.nn.D.tar.gz - for maintenance (MNCL) release

where

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

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

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

Prerequisites

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

Action

At a CS 2000 Management Tools server terminal

1 Make a temporary directory to store the ESD software by typing

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

and pressing the Enter key.

2 Change directory to the newly created location by typing

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

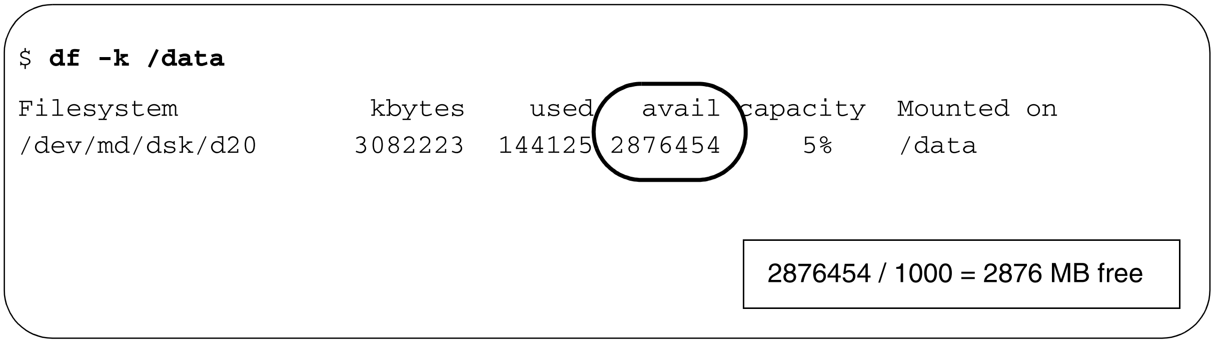
and pressing the Enter key.

3 Ensure that enough disk space is available for the ESD software (500 MByte is recommended) by typing

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

and pressing the Enter key.

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



```
$ df -k /data
Filesystem              kbytes    used   avail capacity  Mounted on
/dev/md/dsk/d20        3082223  144125 2876454     5%    /data
```

2876454 / 1000 = 2876 MB free

4 Transfer the ESD software files from the drop box on the repository server by typing

```
$ ftp <repository_server>
```

and pressing the Enter key.

where

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

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

5 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

6 Retrieve the ESD software load by typing

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

and pressing the Enter key.

where

<esd_filename>
is the ESD filename for the GWC software load

Example
ftp> get GWCC0070.70.V.NCL.NAP.VAULT.8.D.tar.gz

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

7 Repeat step 6 for all ESD software loads recorded in the notification from Nortel Networks.

8 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

9 Extract the ESD software load from the tape archive format by typing

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

and pressing the Enter key.

where

<esd_filename>
is the ESD filename for the GWC software load

Example
$ gtar xvzf GWCC0070.70.V.NCL.NAP.VAULT.8.D.tar.gz

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

10 Access the newly created directory by typing

```
$ cd <esd_filename_directory>
```

and pressing the Enter key.

where

<esd_filename_directory>
is the new directory created to store the extracted software load

Example
$ cd GWCC0070.70.V.NCL.NAP.VAULT.8.D

11 Become the root user by typing

```
$ su - root
```

and pressing the Enter key.

12 When prompted, enter the root password.

13 The ESD software is formatted as an ISO 9660 image. Mount the ISO 9660 image (using the mount_iso.ksh script) by typing

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

and pressing the Enter key.

where

<esd_directory>
is the directory created in step 9

<iso_image>
is the name of the iso image

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

Example
# mount_iso.ksh mount
/data/iso_esd/GWCC0070.70.V.NCL.NAP.VAULT.8D/
GN070_load.iso.tape

A response is printed to the terminal. Use following table to determine if the command was successful.

mount_iso.ksh command responses

Response	Meaning and action
`Is is very important for the user of this command to know that if you mount an iso image. It is a MUST that you umount an image before removing the image file.  If the file is deleted while the OS has it mounted, it can be harmful to the runtime applications on this unit`	This response indicates success.
`Provided full path to ISO image does not exist`	Verify the location and name of the ISO 9660 image, such us /data/iso_esd/GWCC007.../...img.tape, and retry.
`ISO Image Already Mounted`	Enter **mount_iso.ksh umount** to unmount whatever ISO 9660 image is currently mounted, and retry.
`Error creating the image device location`	This response indicates an operating system error with the loopback file driver. Retry the command, and if it fails a second time, contact Nortel Networks support personnel.
`ERROR MOUNTING <ESD_filename>`	This response indicates that either the ISO 9660 file is corrupt, or the `/tmpmnt/noarch` directory has been deleted.

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

14 Use the following table to determine your next step.

If you want to install the software	Do
later	go to step 15
now	go to step 16

15 Copy the contents to a location on the CS 2000 Management Tools server by typing

```
# cp /tmpmnt/noarch/*.* <directory_name>
```

and pressing the Enter key.

where

<directory_name>
is a directory on the CS 2000 Management Tools server, for example /data/iso_esd

Note: Ensure that you have write permission to this directory, and that the same file permissions are set at the old and copied locations.

When installing the software at the later date, complete step 16, but in sub-step e, specify the new location of the software instead of typing /tmpmnt/noarch.

Continue with step 23.

16 Complete the following steps to install the software on the CS 2000 Core Manager or CBM.

a List the contents of the /tmpmnt/noarch directory by typing

```
# ls /tmpmnt/noarch
```

and pressing the Enter key.

Record the name of the .rpm file.

b Execute the installation script by typing

```
# platform_load_install.sh
```

and pressing the Enter key.

c When prompted, select the option "Install RPM from Disk" by typing

```
> 2
```

and pressing the Enter key.

d When prompted, enter the .rpm filename and press the Enter key.

e When prompted, enter the location of the .rpm file by typing

```
# /tmpmnt/noarch
```

and pressing the Enter key.

The system installs the software on the CS 2000 Core Manager or CBM.

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

f Exit the installation program by typing

```
# x
```

and pressing the Enter key.

If your office is configured with a	Do
CS 2000 Core Manager	go to step 17
CBM	go to step 23

At the CS 2000 Core Manager console or terminal window

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

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

18 Access the gwc directory by typing

```
# cd /swd/gwc
```

and pressing the Enter key.

19 Execute the GwcConfig.sh script by typing

```
# ./GwcConfig.sh
```

and pressing the Enter key.

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

20 If prompted, enter the hostname of the SAM21 EM server and press the Enter key. Otherwise, continue with step 22.

21 If prompted, enter the IP address of the SAM21 EM server and press the Enter key. Otherwise, continue with step 22.

22 Log out of the CS 2000 Core Manager by typing

```
# exit
```

and pressing the Enter key.

At a CS 2000 Management Tools server terminal

23 Unmount the ESD file by typing

```
# mount_iso.ksh umount
```

and pressing the Enter key.

24 This procedure is complete.

Create a backup of the GWC load file

Purpose of this procedure

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

When to use this procedure

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

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

Prerequisites

There are no prerequisites to this procedure.

Action

At the CS 2000 Core Manager or CBM console

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

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

2 Change directory to the GWC software directory by typing

# cd /swd/gwc

and pressing the Enter key.

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

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

> ***Note:*** There will likely be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of a specific GWC card or node, refer to procedure "View the operational status of a GWC" found in the Gateway

Controller Configuration Management NTP, NN10205-511, to locate the load filename associated with a specific GWC card.

5

> **CAUTION**
>
> Be sure to use the command **cp** in this step.
>
> Failure to use the **cp** command can cause problems with the general upgrade process.

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

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

and pressing the Enter key.

where

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

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

6 Change the permissions for the image file by typing

```
# chmod 755 <load_filename>.imag.bak
```

and pressing the Enter key.

where

<load_filename>
is the GWC load filename

7 The procedure is complete.

Note: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 4.

View the contents of a load file image

Purpose of this procedure

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

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

When to use this procedure

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

Use this procedure to determine if delivered load contains patches.

Prerequisites

This procedure has no prerequisites.

Action

Use the following table to determine your first step.

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

At the CS 2000 Management Tools server

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

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

and pressing the Enter key.

2 List all the GWC load names by typing

```
# ls
```

and pressing the Enter key.

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

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

and pressing the Enter key.

where

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

Example response:

```
Load information from pgc09bl_patched_03_04.imag

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

Patch-ID    Status    Activation

XBN63GZ9    Applied   NonAct

XED41GZ9    Applied   NonAct

XQA89GZ9    Applied   NonAct

.

.

.
```

4 This procedure is complete.

Note: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 4.

At the CS 2000 Management Tools terminal

5 Access the temporary directory by typing

```
# cd /tmp
```

and pressing the Enter key.

6 Access the CBM server by typing

```
# ftp <CBM_IP_address>
```

and pressing the Enter key.

where

<CBM_IP_address>
is the IP address of the CBM server

7 When prompted, enter the user name by typing

```
Name: gwcload
```

and pressing the Enter key.

8 When prompted, enter the password by typing

```
Password: gwcload
```

and pressing the Enter key.

9 Set up the ftp transfer process to binary by typing

```
ftp> bin
```

and pressing the Enter key.

10 Transfer the GWC image load file by typing

```
ftp> get <gwc_image_name>
```

and pressing the Enter key.

where

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

Example response:

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

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

```
ftp> quit
```

and pressing the Enter key.

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

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

and pressing the Enter key.

where

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

Example response:

```
Load information from pgt93ax.imag

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

Patch-ID    Status    Activation

XBN63GZ9    Applied   NonAct

XED41GZ9    Applied   NonAct

XQA89GZ9    Applied   NonAct

.

.

.
```

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

```
# rm /tmp/<gwc_image_name>
```

and pressing the Enter key.

where

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

14 This procedure is complete.

Note: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 4.

Upgrade a standby GWC card software load

Purpose of this procedure

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

When to use this procedure

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

Prerequisites and guidelines

CAUTION

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

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

- Install GWC package onto the CS 2000 Core Manager or CBM from CD-ROM on page 23
- Deliver and install GWC package using Electronic Software Delivery on page 28

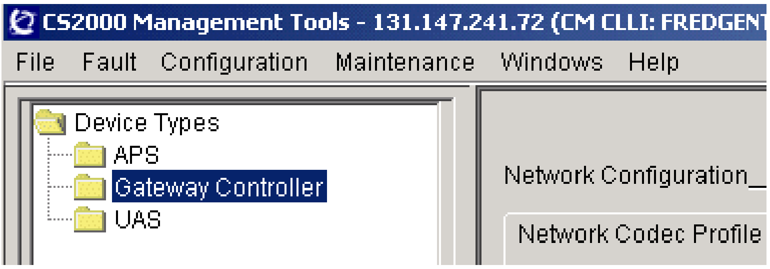
While upgrading the software on a GWC card, the port on the LAN router connected to the GWC card must be set to the Ethernet parameter of “auto-negotiate”. This action must be performed after the card is locked and before the card is unlocked. Refer to step 9 in this procedure.

If the Communications Server LAN (CS LAN) is provided by Nortel Networks Passport 8000 series router switches, refer to Re-provision Passport port to auto-negotiate on page 55 for a procedure to reconfigure the port on the CS LAN router to “auto-negotiate”.

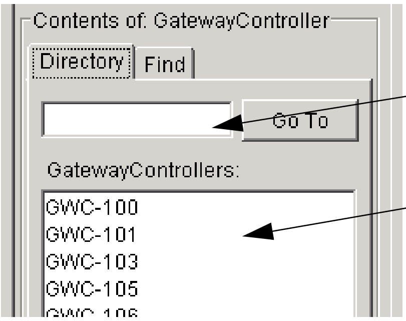
Action

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.

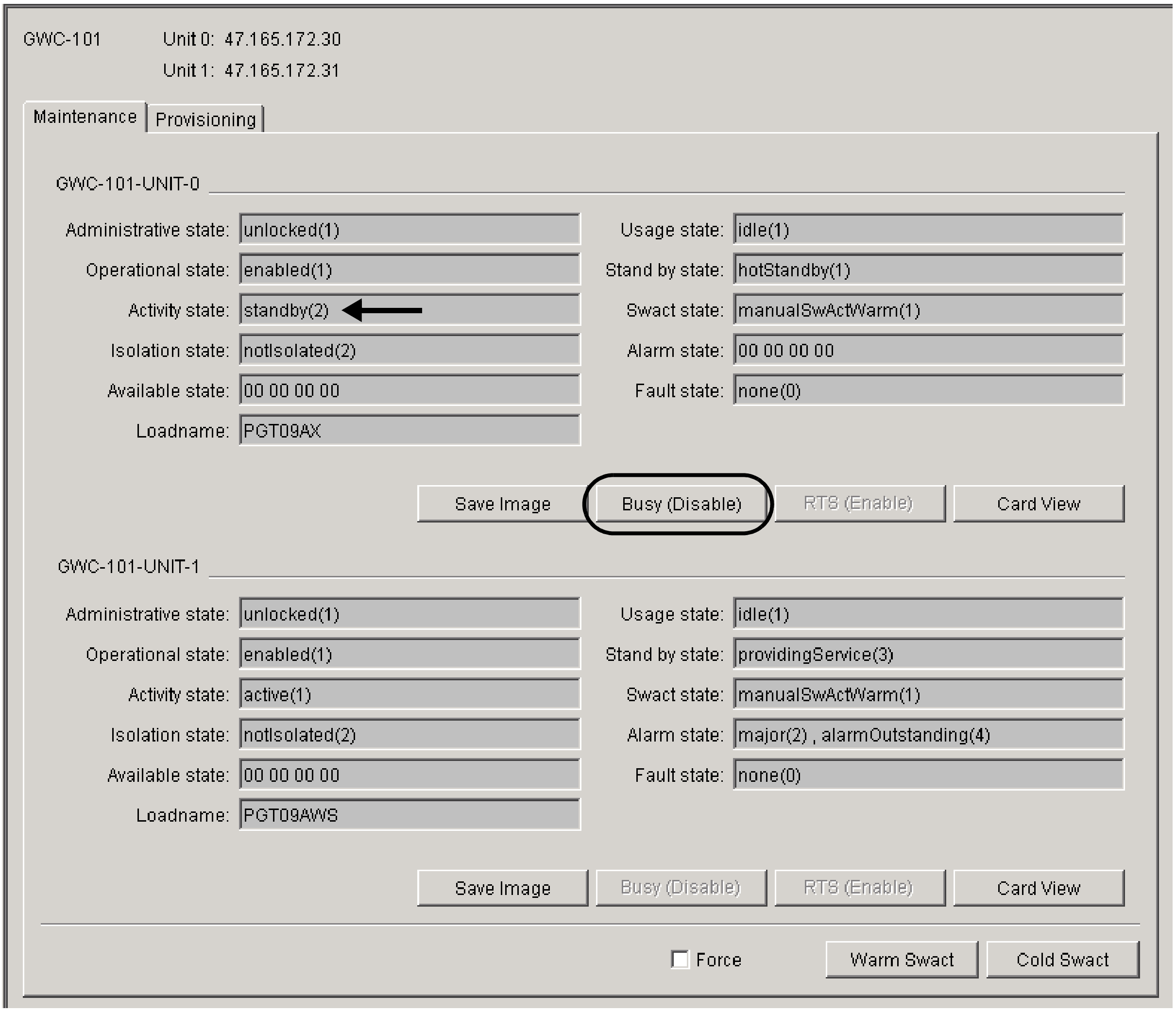


Type a GWC node number here

or

Select a GWC node from the list of provisioned GWC nodes

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



GWC-101 Unit 0: 47.165.172.30

Unit 1: 47.165.172.31

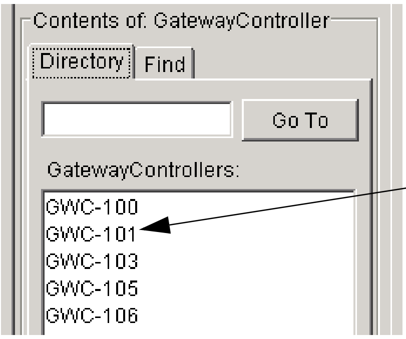
GWC-101-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGT09AX		

GWC-101-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGT09AWS		

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.



GatewayControllers:

GWC-100
GWC-101
GWC-103
GWC-105
GWC-106

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

5 Use the following table to determine your next step.

If	Do
you need to re-provision the port on the Passport switch to “auto-negotiate” (the CS LAN is provided by Nortel Networks Passport 8000 series router switches)	go to step 6
otherwise	go to step 7

At the CLI for the Passport

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

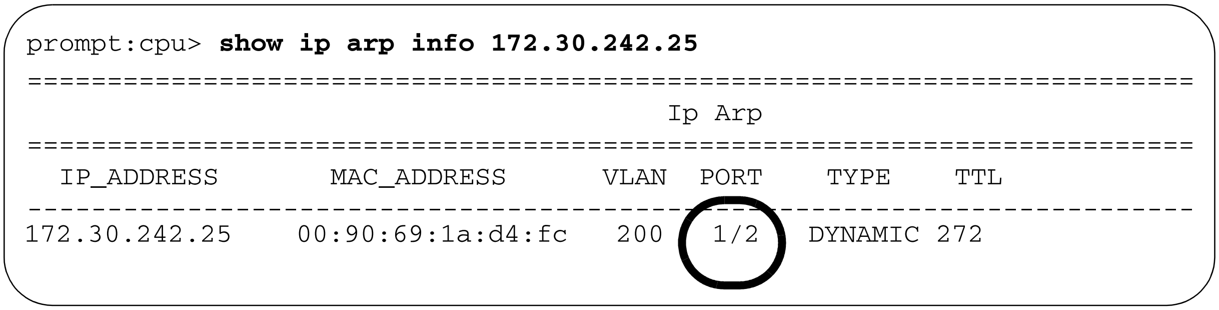
> show ip arp info <ip_address>

and pressing the Enter key.

ip_address
is the physical IP address of the GWC card.

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

Example response:

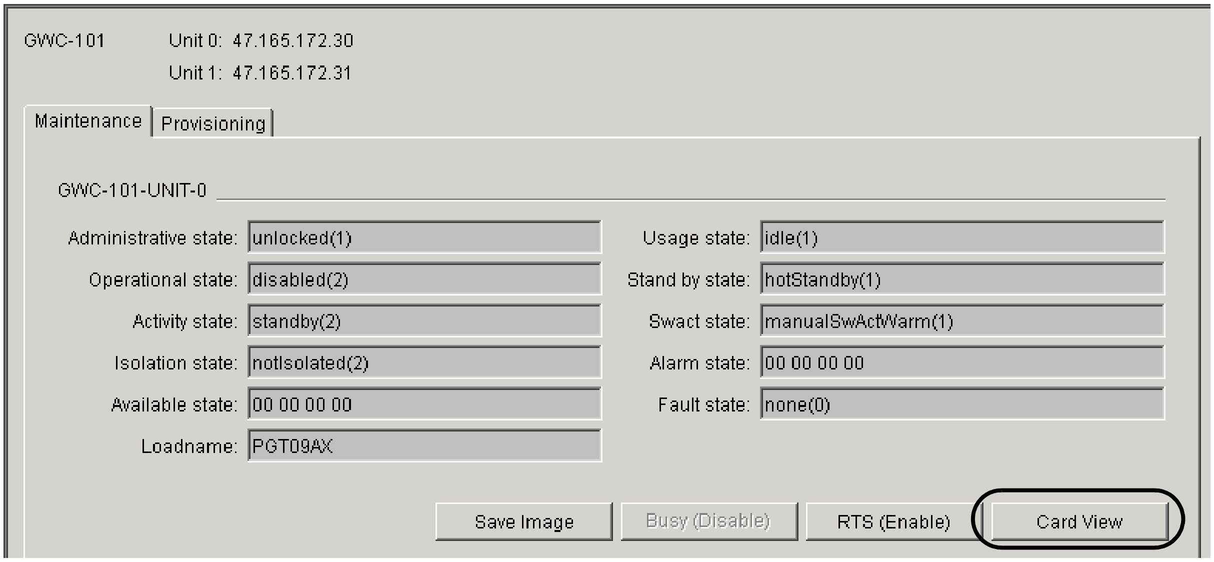


```
prompt:cpu> show ip arp info 172.30.242.25
==========================================================================
                                        Ip Arp
==========================================================================
  IP_ADDRESS       MAC_ADDRESS       VLAN   PORT     TYPE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

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

At the CS 2000 GWC Manager client

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



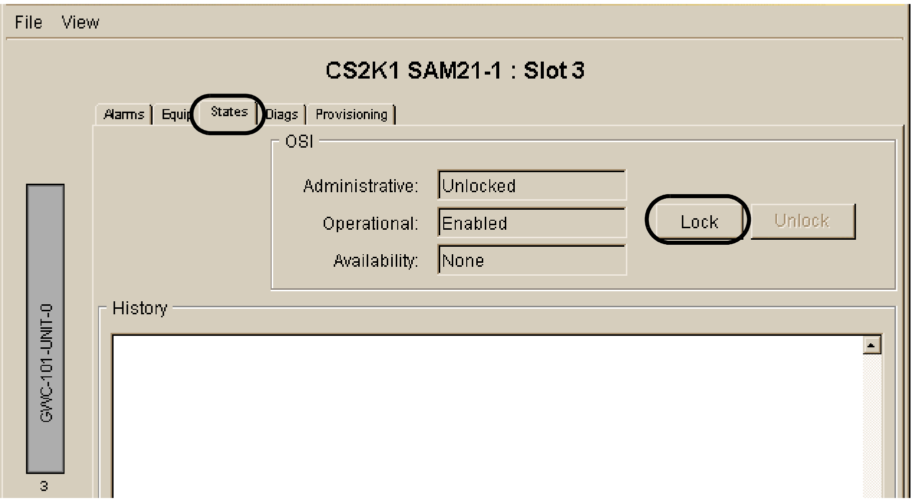
GWC-101 Unit 0: 47.165.172.30
Unit 1: 47.165.172.31

GWC-101-UNIT-0

Administrative state: unlocked(1)
Operational state: disabled(2)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: PGT09AX
Usage state: idle(1)
Stand by state: hotStandby(1)
Swact state: manualSwActWarm(1)
Alarm state: 00 00 00 00
Fault state: none(0)

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.



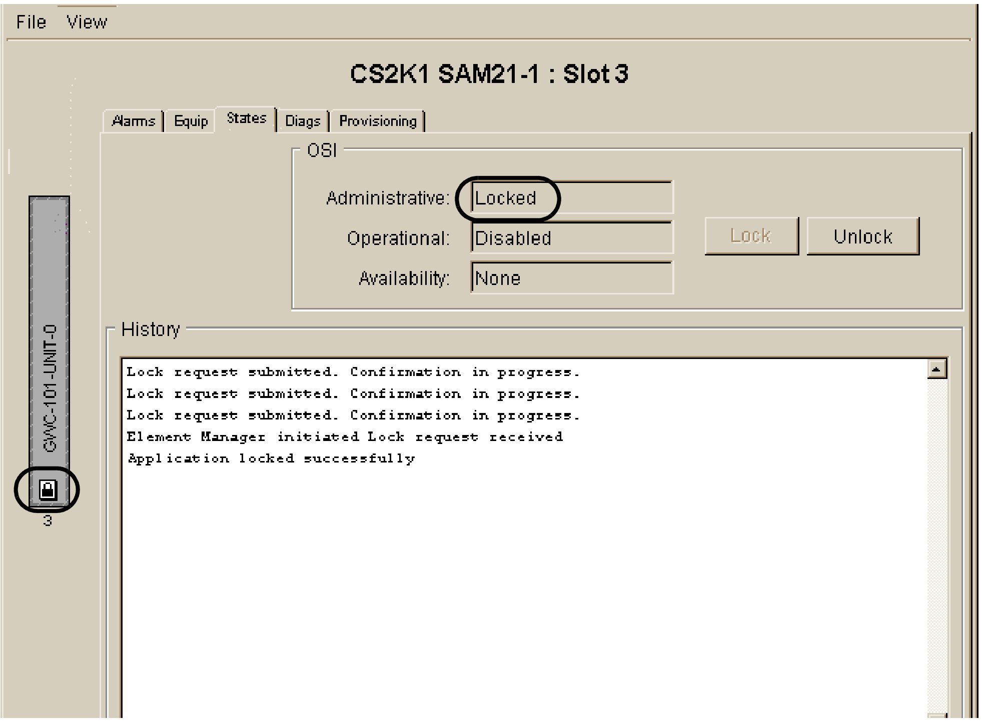
CS2K1 SAM21-1 : Slot 3

OSI
Administrative: Unlocked
Operational: Enabled
Availability: None

History

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

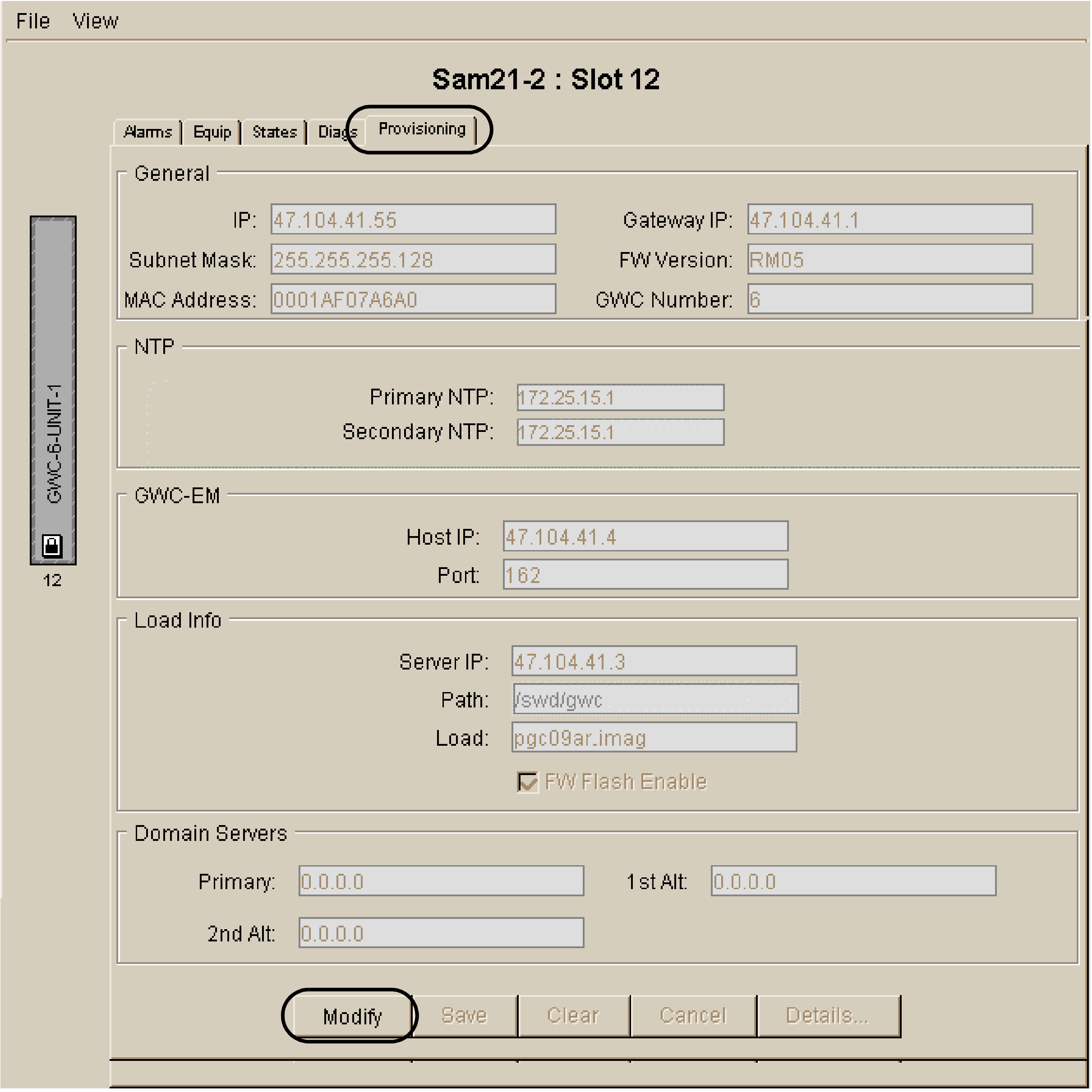
> ***Note:*** If the CS LAN is provided by Nortel Networks Passport 8000 series router switches, re-provision the port on the Passport switch to “auto-negotiate”. Refer to Re-provision Passport port to auto-negotiate on page 55.



Administrative: Locked
Operational: Disabled
Availability: None

```
Lock request submitted. Confirmation in progress.
Lock request submitted. Confirmation in progress.
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

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



Sam21-2 : Slot 12

General

IP: 47.104.41.55

Subnet Mask: 255.255.255.128

MAC Address: 0001AF07A6A0

Gateway IP: 47.104.41.1

FW Version: RM05

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: pgc09ar.imag

☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

11

CAUTION

The Path: field must be set to /swd/gwc.

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

Type the new load file name in the **Load:** field.

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

12 Use the following table to determine your next step.

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

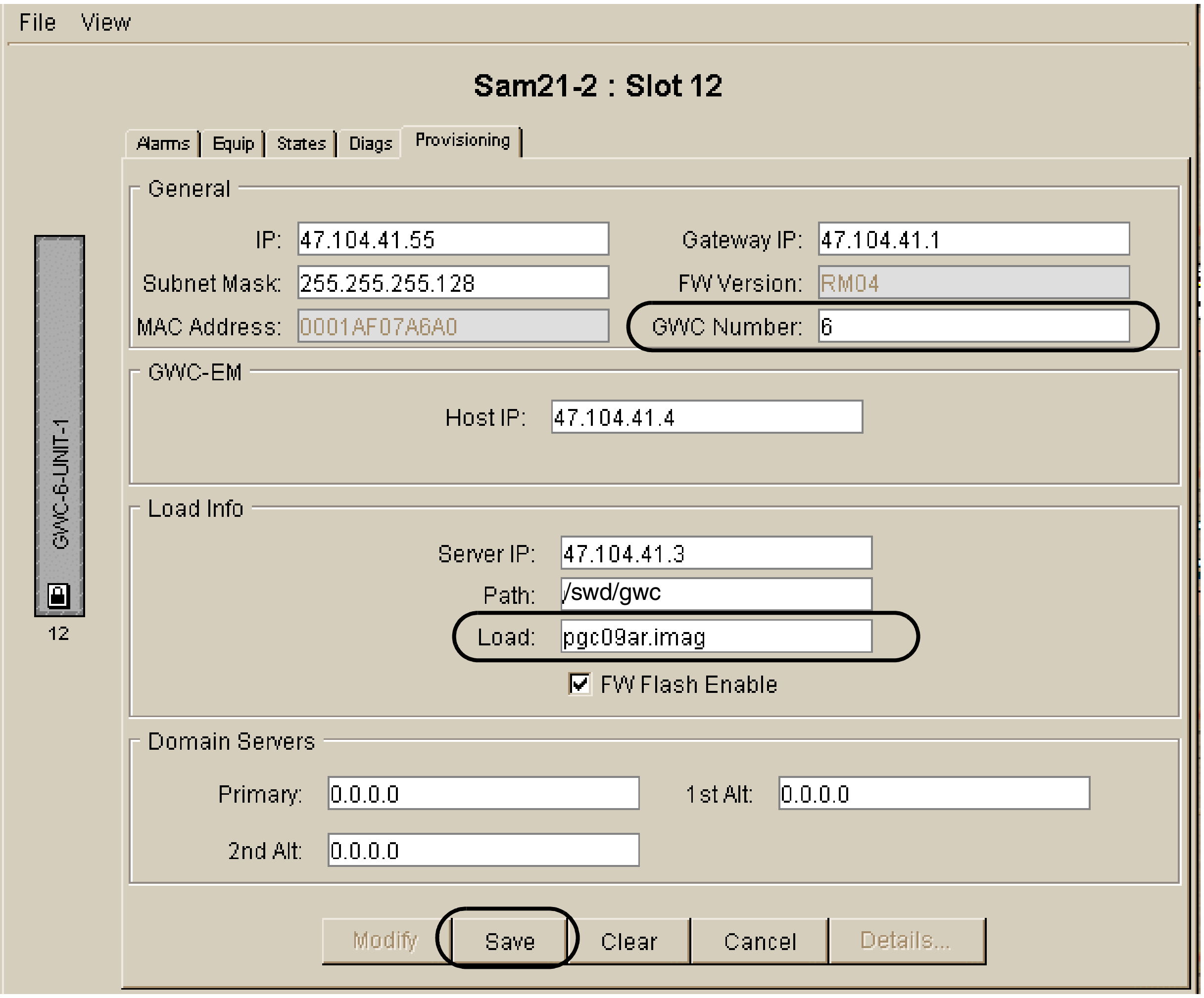
13 Type the GWC number in the **GWC Number:** field that you recorded in step 4. Refer to the following figure to locate these fields.

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

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

14 Click the **Save** button.

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



Sam21-2 : Slot 12

General

IP: 47.104.41.55

Subnet Mask: 255.255.255.128

MAC Address: 0001AF07A6A0

Gateway IP: 47.104.41.1

FW Version: RM04

GWC Number: 6

GWC-EM

Host IP: 47.104.41.4

Load Info

Server IP: 47.104.41.3

Path: /swd/gwc

Load: pgc09ar.imag

☑ FW Flash Enable

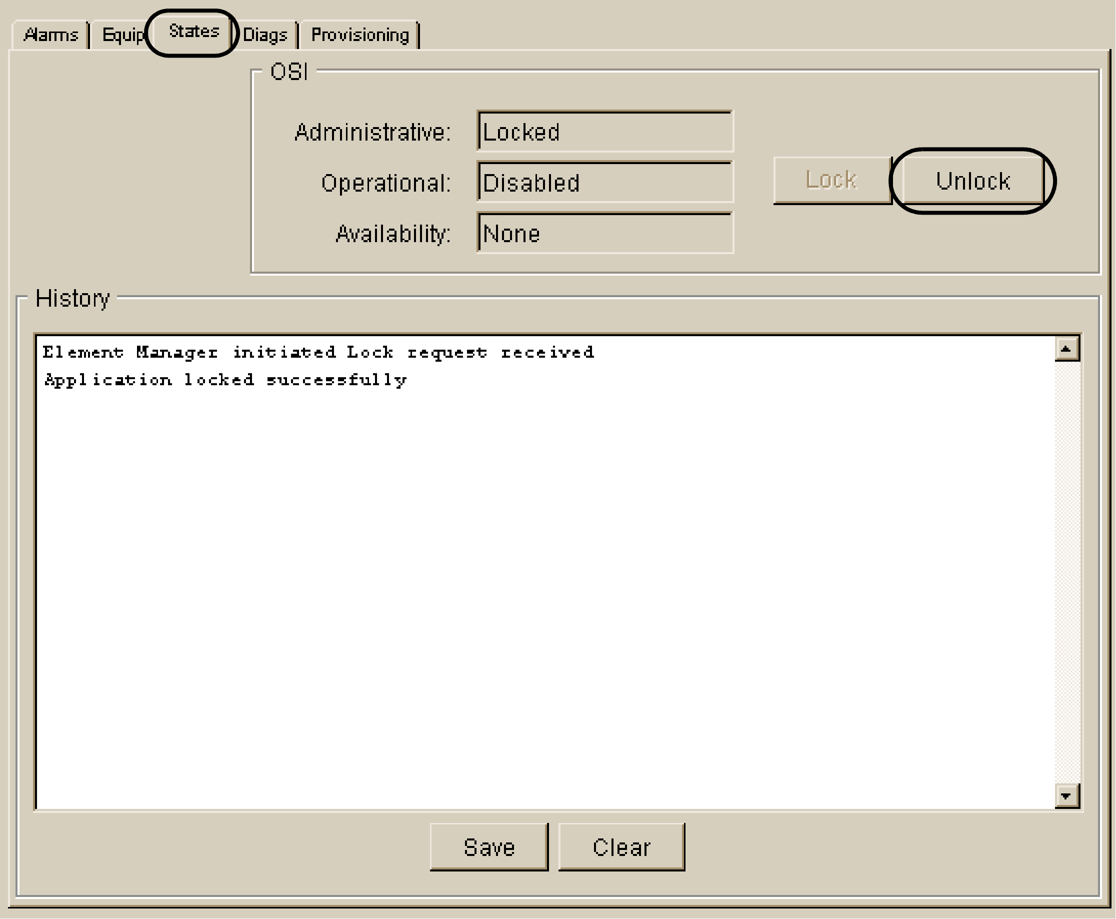
Domain Servers

Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

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



Administrative: Locked

Operational: Disabled

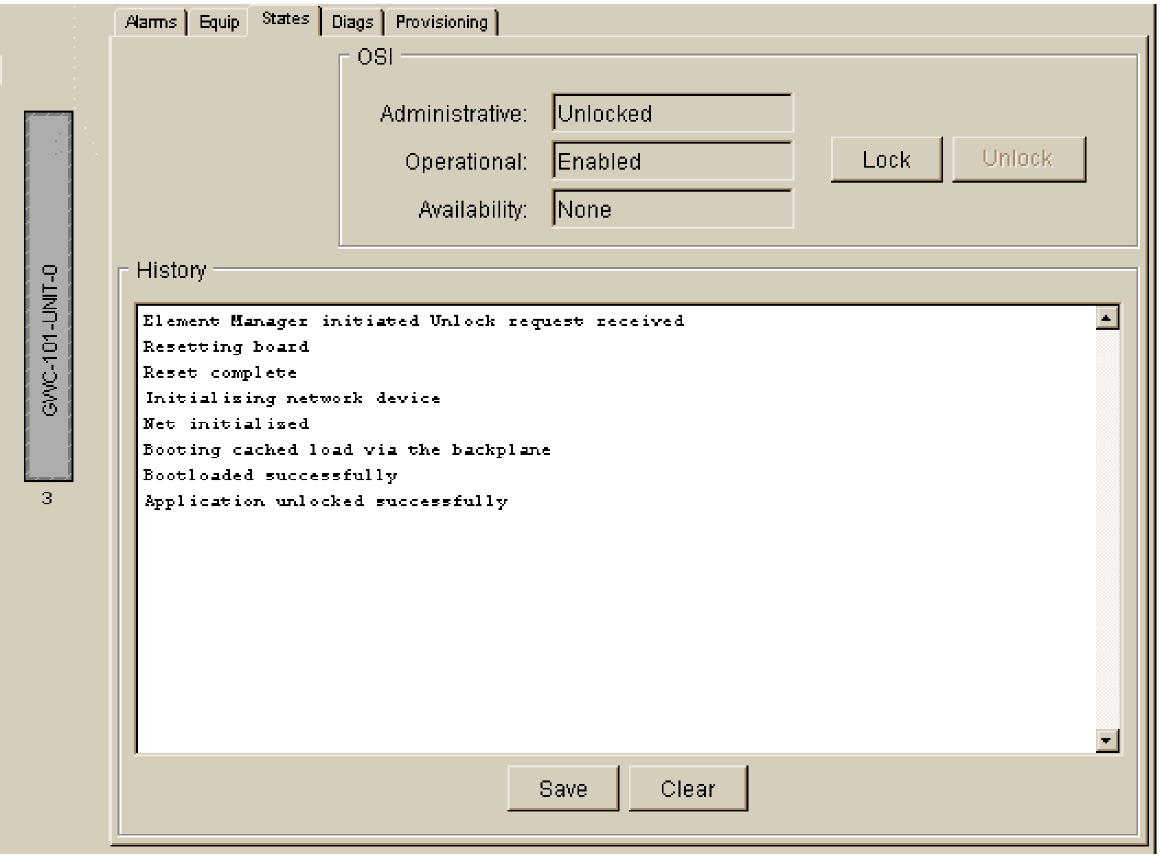
Availability: None

```
Element Manager initiated Lock request received
Application locked successfully
```

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.



OSI

Administrative: Unlocked

Operational: Enabled

Availability: None

History

```
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

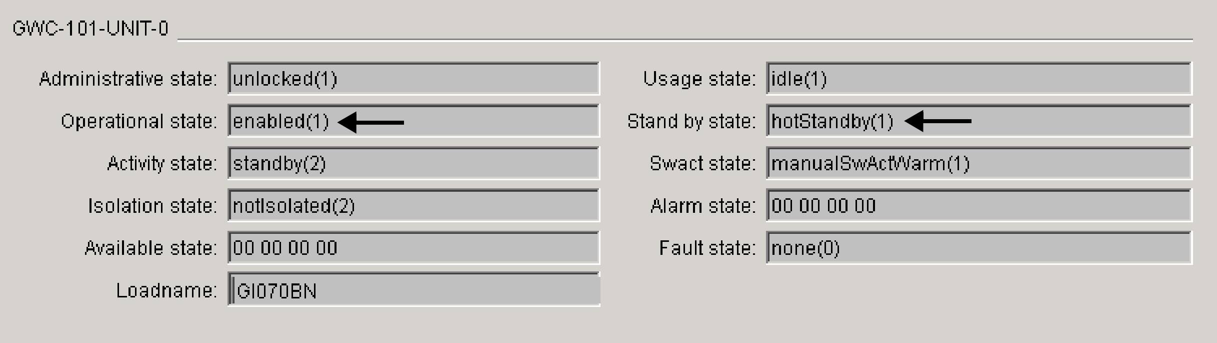
At the CS 2000 GWC Manager

18 Determine the next action to take.

If patching	Do
is needed but has not been completed	perform the following procedures in the order listed, then continue with step 15: Transfer patches to the NPM database manually on page 89, Apply patches using the NPM on page 101, Activate patches using the NPM on page 110 Take a manual GWC software image on page 141;
has been completed	continue with step 19
is not needed	continue with step 19

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

If the inactive GWC does not come into an Operational State of “enabled” and a Standby state of “hotstandby”, then refer to the section “GWC does not RTS” in the procedure Troubleshoot GWC upgrades on page 162 in this NTP. If error recovery fails, stop this procedure and contact your next level of support.



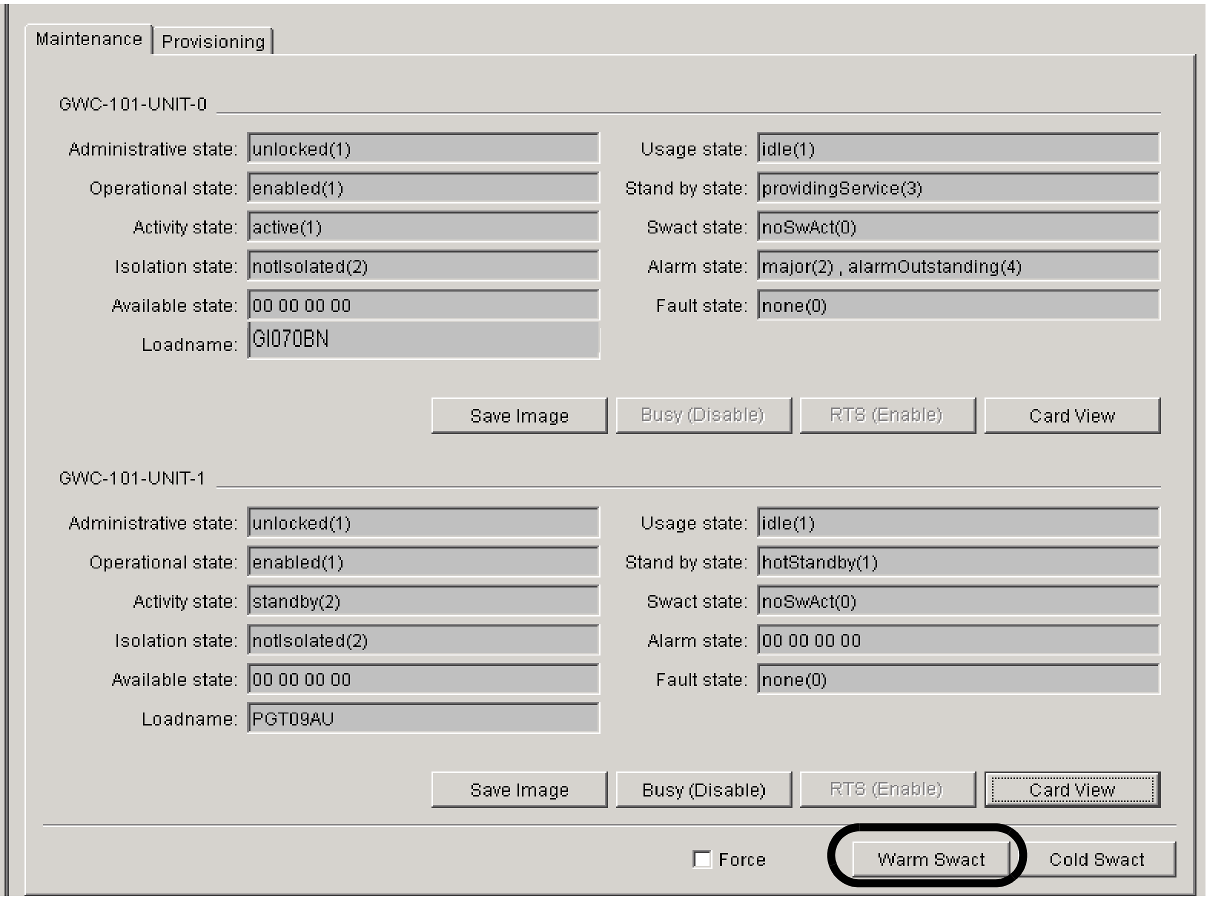
GWC-101-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

At the CS 2000 GWC Manager

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

> ***Note:*** If the SwAct fails or the inactive unit does not RTS in 1 minute, then refer to the section “Warm SwAct Failed” in the procedure Troubleshoot GWC upgrades on page 162 in this NTP.
>
> If the GWC card does not successfully execute a warm SwAct using the Troubleshooting procedure, then perform the procedure Rollback a software upgrade on a standby GWC on page 57 in this NTP.



GWC-101-UNIT-0

Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: active(1)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GI070BN
Usage state: idle(1)
Stand by state: providingService(3)
Swact state: noSwAct(0)
Alarm state: major(2) , alarmOutstanding(4)
Fault state: none(0)

GWC-101-UNIT-1

Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: PGT09AU
Usage state: idle(1)
Stand by state: hotStandby(1)
Swact state: noSwAct(0)
Alarm state: 00 00 00 00
Fault state: none(0)

21 Determine your next action:

If you need to upgrade	Do
the mate GWC card (now the new standby GWC card) in the same node	step 3 and complete this procedure
cards in another GWC node	step 2 and complete this procedure

Note: Otherwise, proceed to the next step. You only need to perform this procedure once for each card in a GWC node.

22 The procedure is complete.

Note: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 4.

Re-provision Passport port to auto-negotiate

To enable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch.

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

At the CLI for the Passport

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

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

and pressing the Enter key.

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

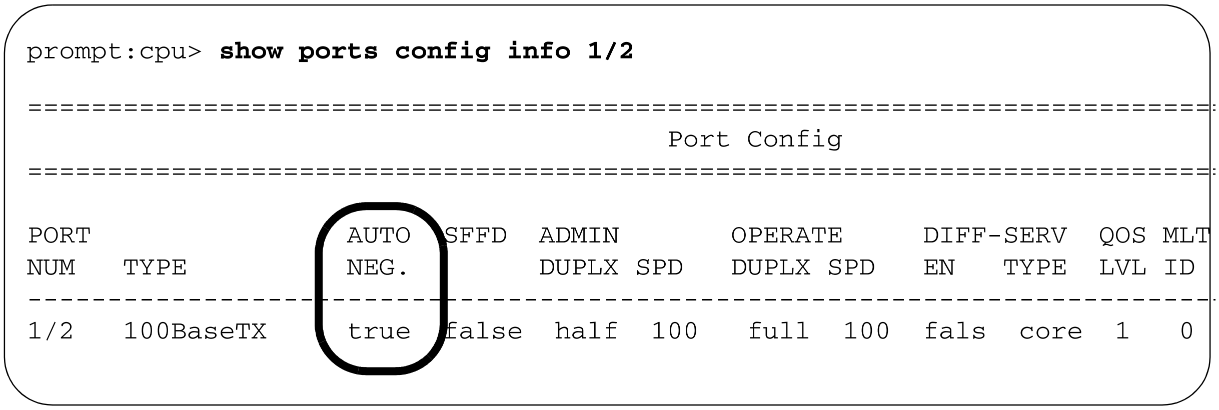
```
prompt:cpu> config ethernet 1/2 auto-negotiate enable
prompt:cpu>
```

2 Verify the port configuration by typing

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

and pressing the Enter key.

The slot and port configuration is displayed.



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

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

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

3 Commit the change by typing

> save config

and pressing the Enter key.

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

Rollback a software upgrade on a standby GWC

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 19, 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

A GWC software load file from a previous release or a backup image file must be available on the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM).

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.

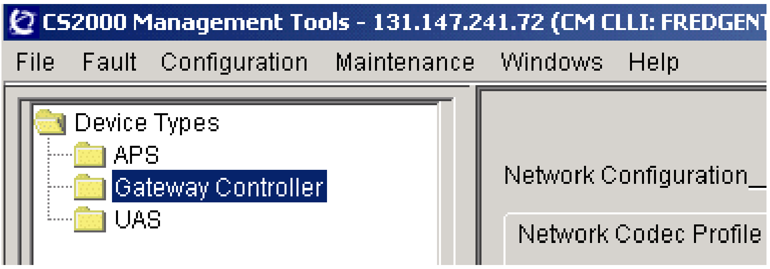
CAUTION

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

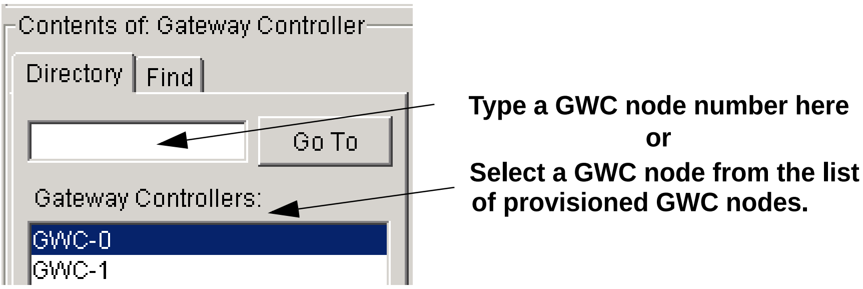
Action

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.

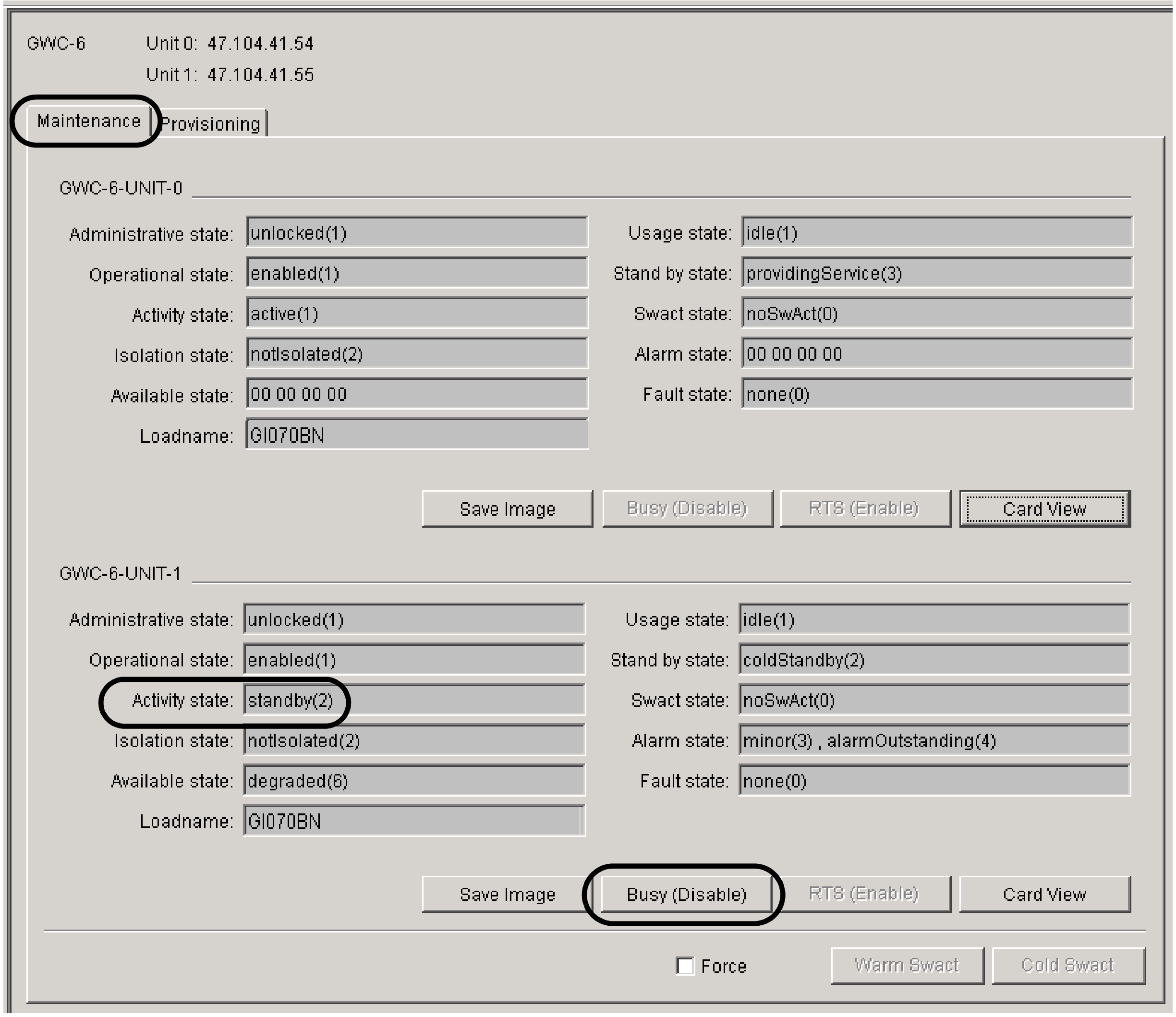


2 From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to roll back.



Type a GWC node number here
or
Select a GWC node from the list of provisioned GWC nodes.

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.



GWC-6 Unit 0: 47.104.41.54
Unit 1: 47.104.41.55

GWC-6-UNIT-0

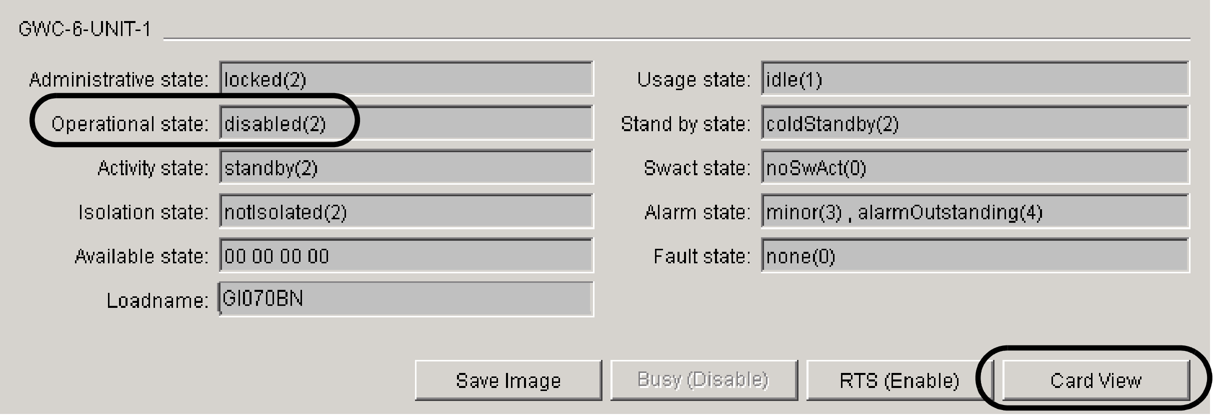
Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

GWC-6-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	coldStandby(2)
Activity state:	standby(2)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	minor(3) , alarmOutstanding(4)
Available state:	degraded(6)	Fault state:	none(0)
Loadname:	GI070BN		

☐ Force

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.



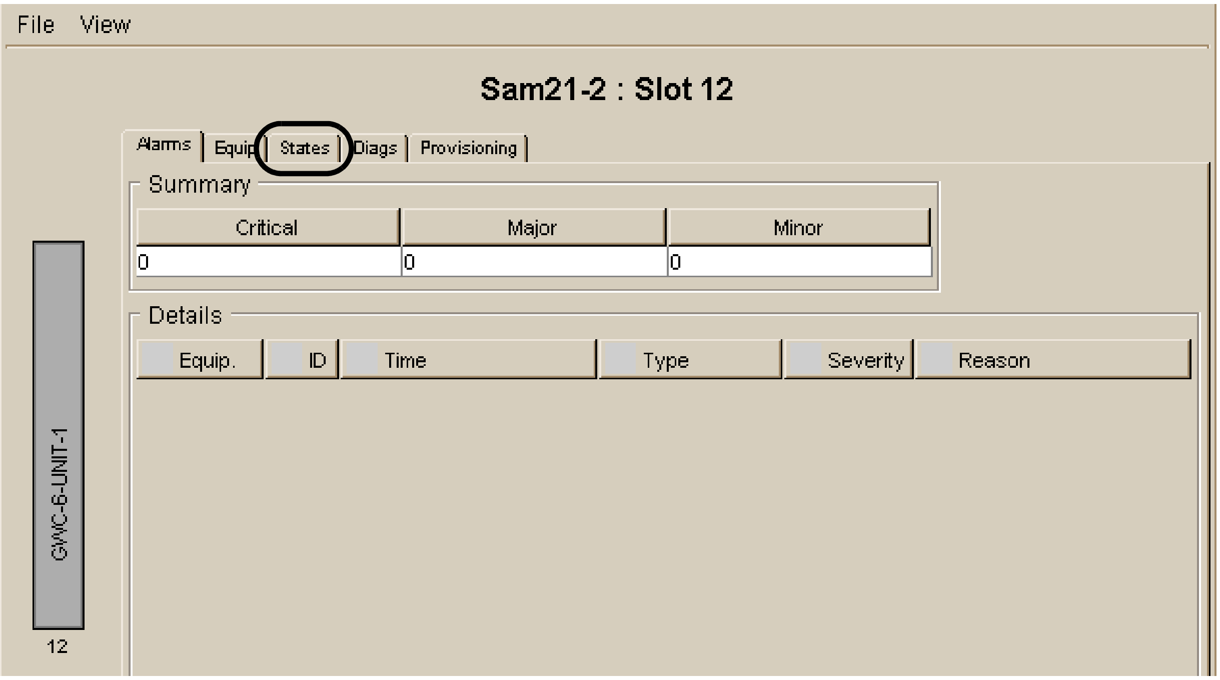
GWC-6-UNIT-1

Administrative state: locked(2)
Operational state: disabled(2)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GI070BN

Usage state: idle(1)
Stand by state: coldStandby(2)
Swact state: noSwAct(0)
Alarm state: minor(3) , alarmOutstanding(4)
Fault state: none(0)

At the CS 2000 SAM21 Manager client

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



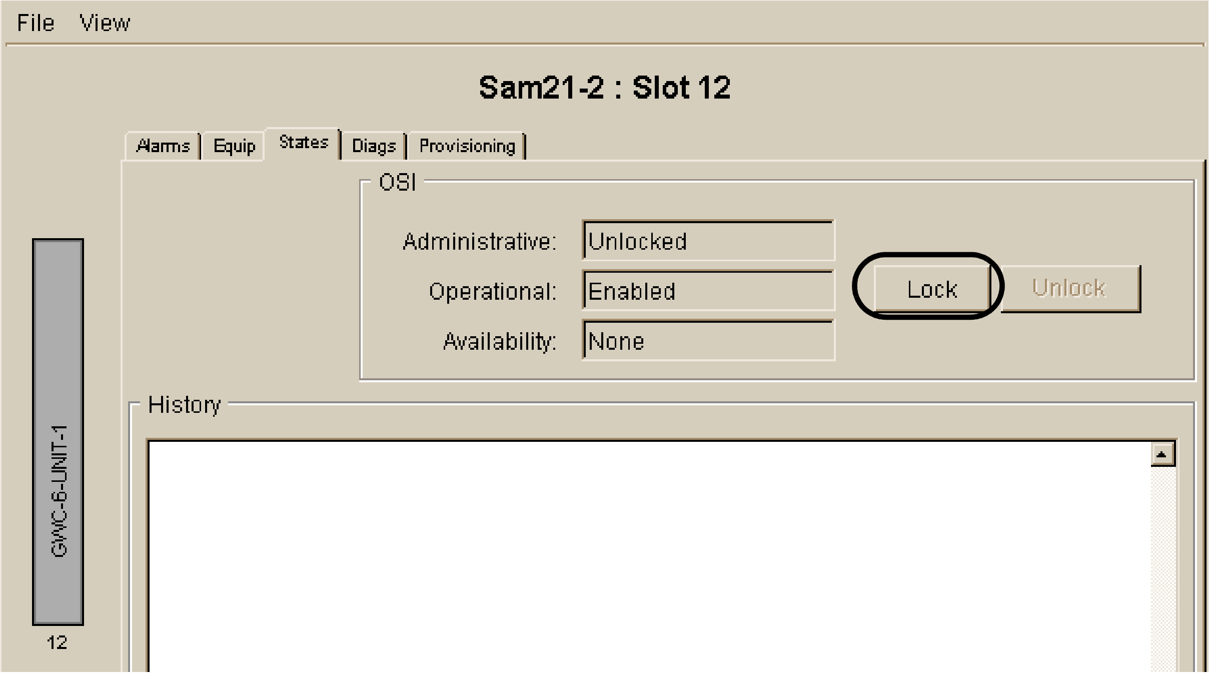
Summary

Critical	Major	Minor
0	0	0

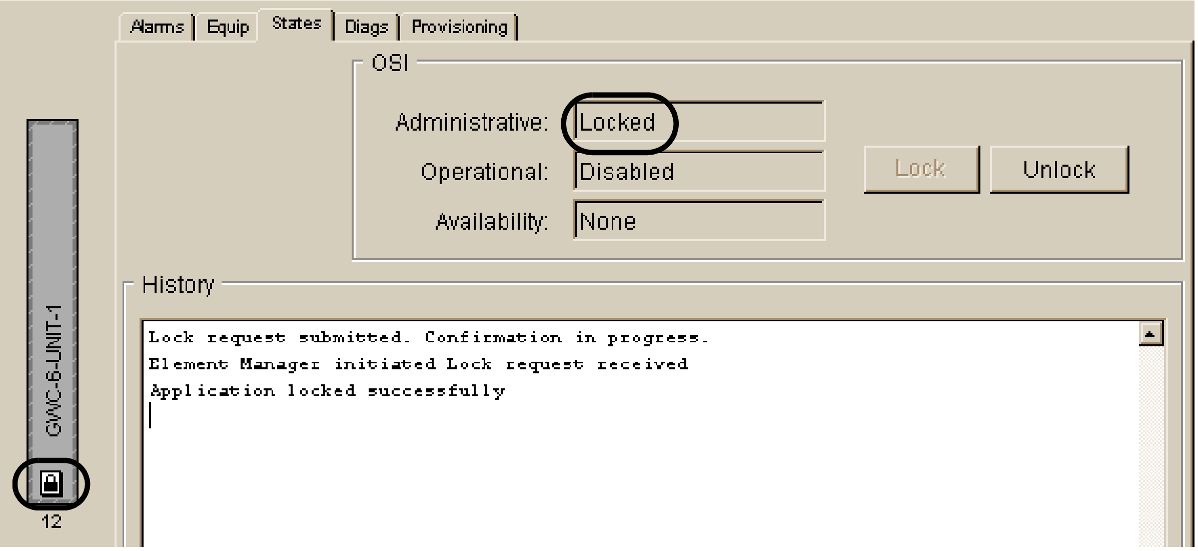
Details

Equip.	ID	Time	Type	Severity	Reason

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 Administrative state "Locked".



Administrative: Unlocked
Operational: Enabled
Availability: None



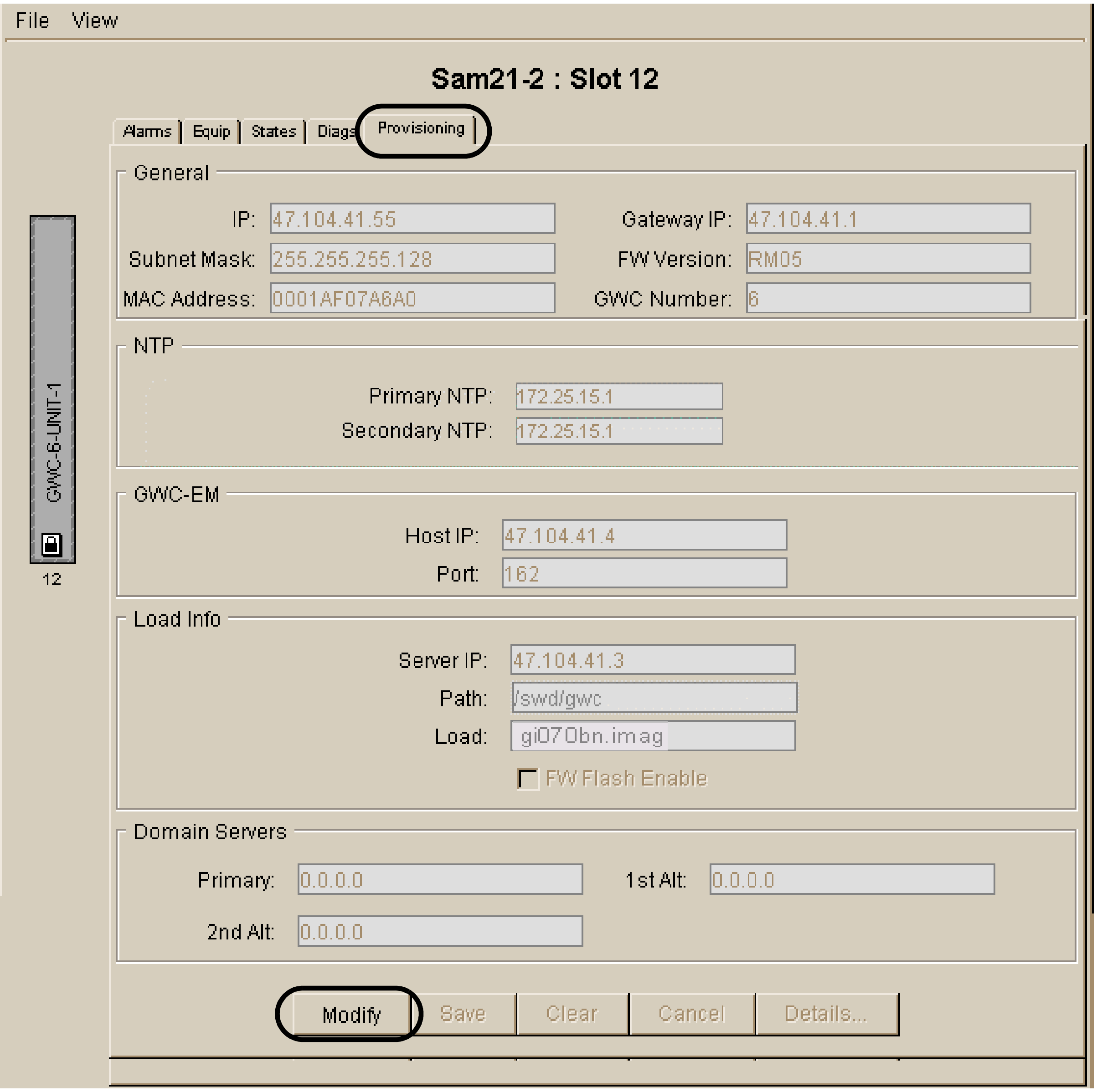
Administrative: Locked
Operational: Disabled
Availability: None

```
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

7 If the CS LAN is provided by Nortel Networks Passport 8000 series router switches and you are downgrading to the SN05 load, reprovision the port on the Passport switch to disable auto-negotiate. Refer to Reprovision Passport port to disable auto-negotiate on page 67.

Otherwise, continue with step 8.

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



Sam21-2 : Slot 12

General

IP: 47.104.41.55
Gateway IP: 47.104.41.1
Subnet Mask: 255.255.255.128
FW Version: RM05
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
□ FW Flash Enable

Domain Servers

Primary: 0.0.0.0
1st Alt: 0.0.0.0
2nd Alt: 0.0.0.0

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

10 Telnet to the CS 2000 Core Manager or CBM and log in as the root user.

> ***Note:*** Telnet to the CS 2000 Core Manager or CBM, or access the CS 2000 Core Manager or CBM console and log in as the root user.

11 List the GWC load files in the /swd/gwc directory.

Example
# ls /swd/gwc

Example of system response:

```
pgc09au.imag
pgc09av.imag
pgc09aw.imag
```

12

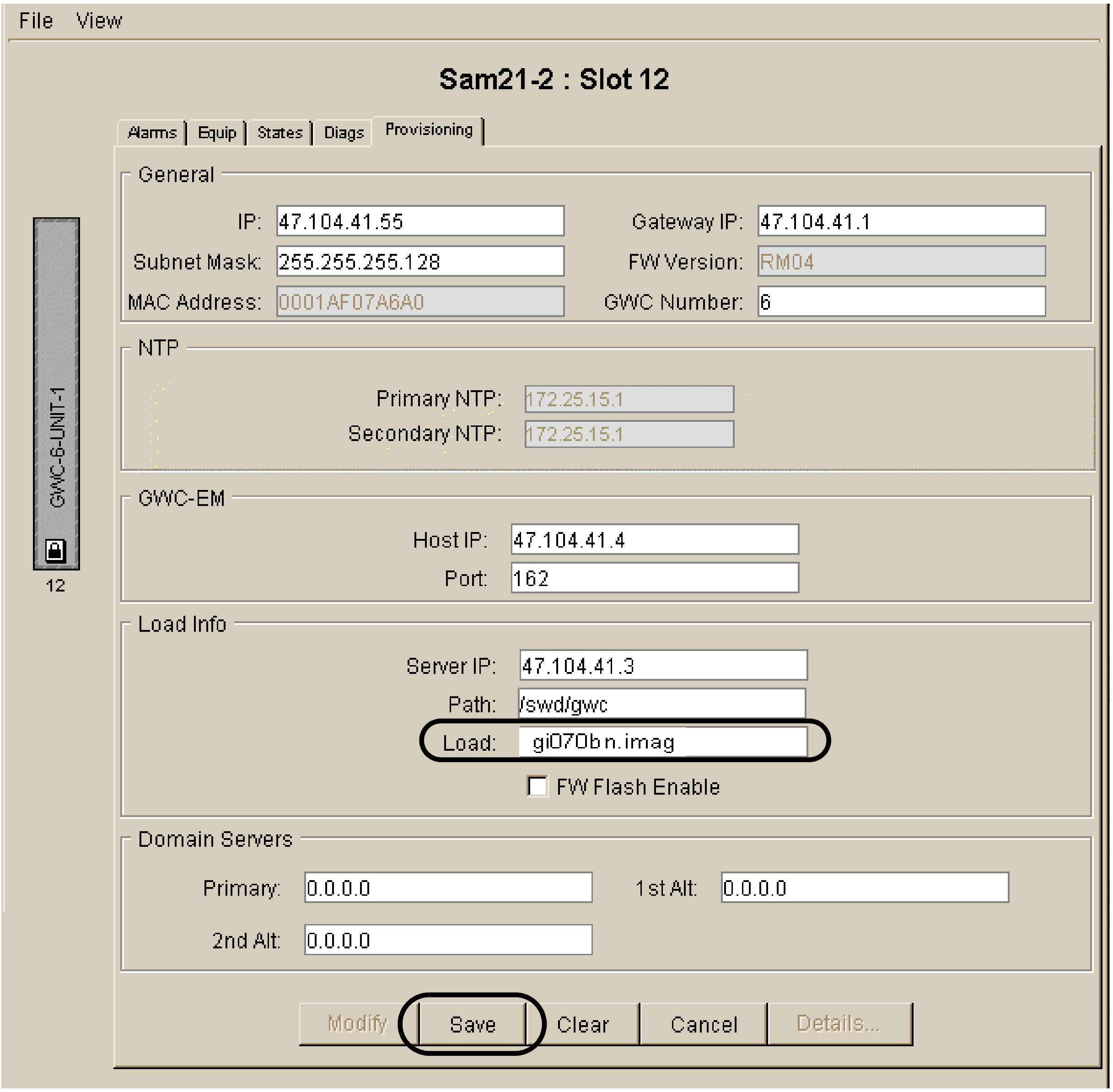
CAUTION

In this step, the Path: field must be set to /swd/gwc.

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

Enter the load file name to revert to from the list you displayed during step 11 and then click the **Save** button.

> ***Note:*** Leave the F/W (firmware) Flash Enable checkbox unselected.



Sam21-2 : Slot 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

☐ FW Flash Enable

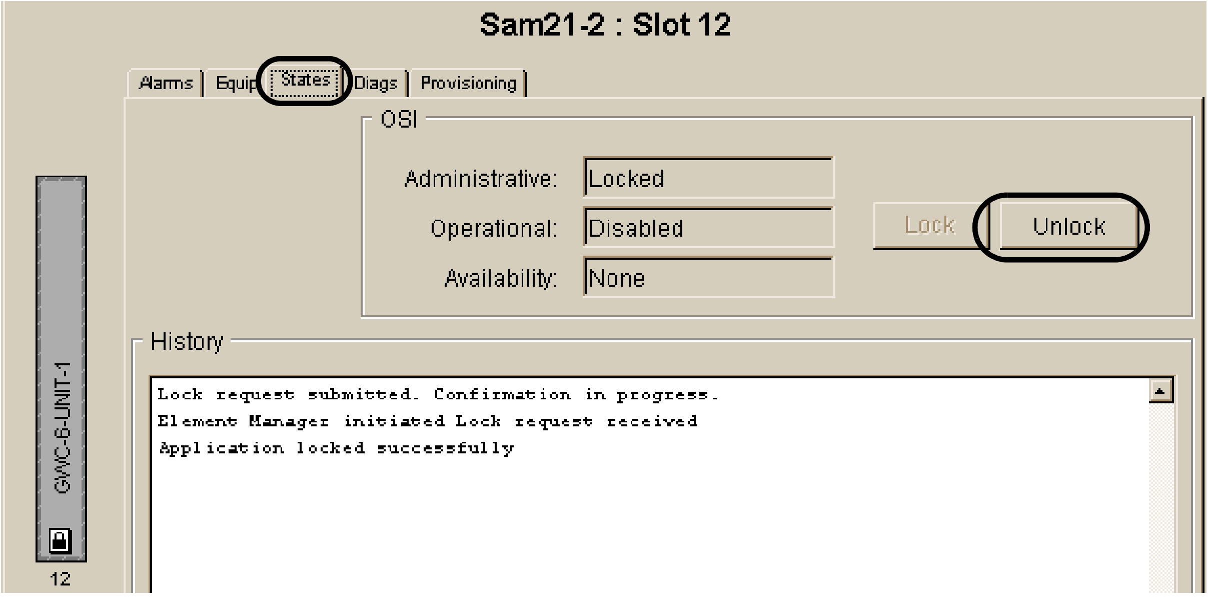
Domain Servers

Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

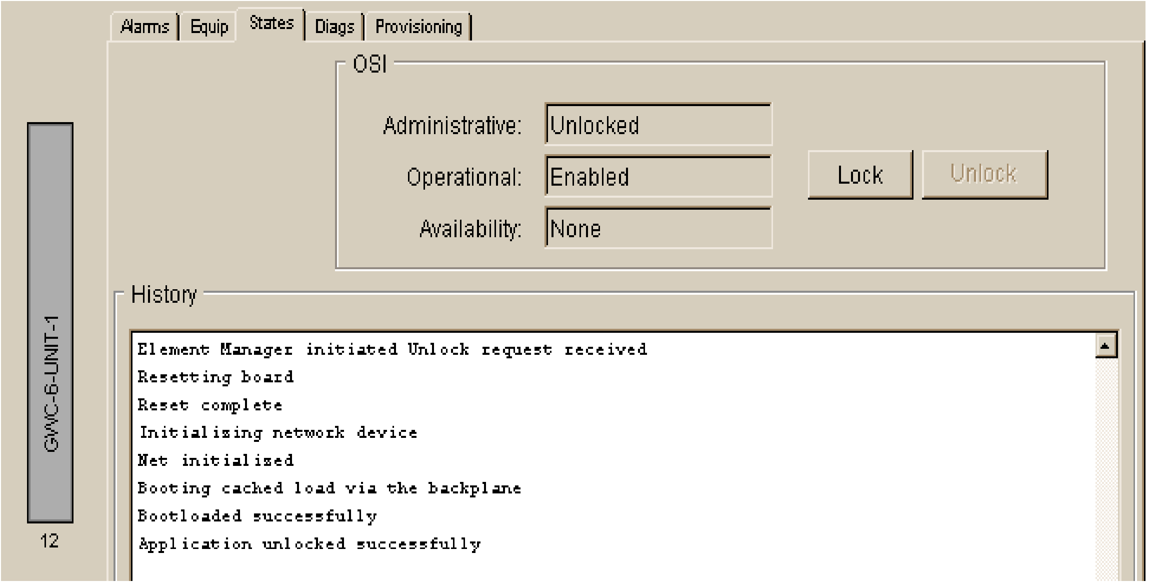
13 Select the **States** tab in the card view.



Administrative: Locked
Operational: Disabled
Availability: None

```
Lock request submitted. Confirmation in progress.
Element Manager initiated Lock request received
Application locked successfully
```

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



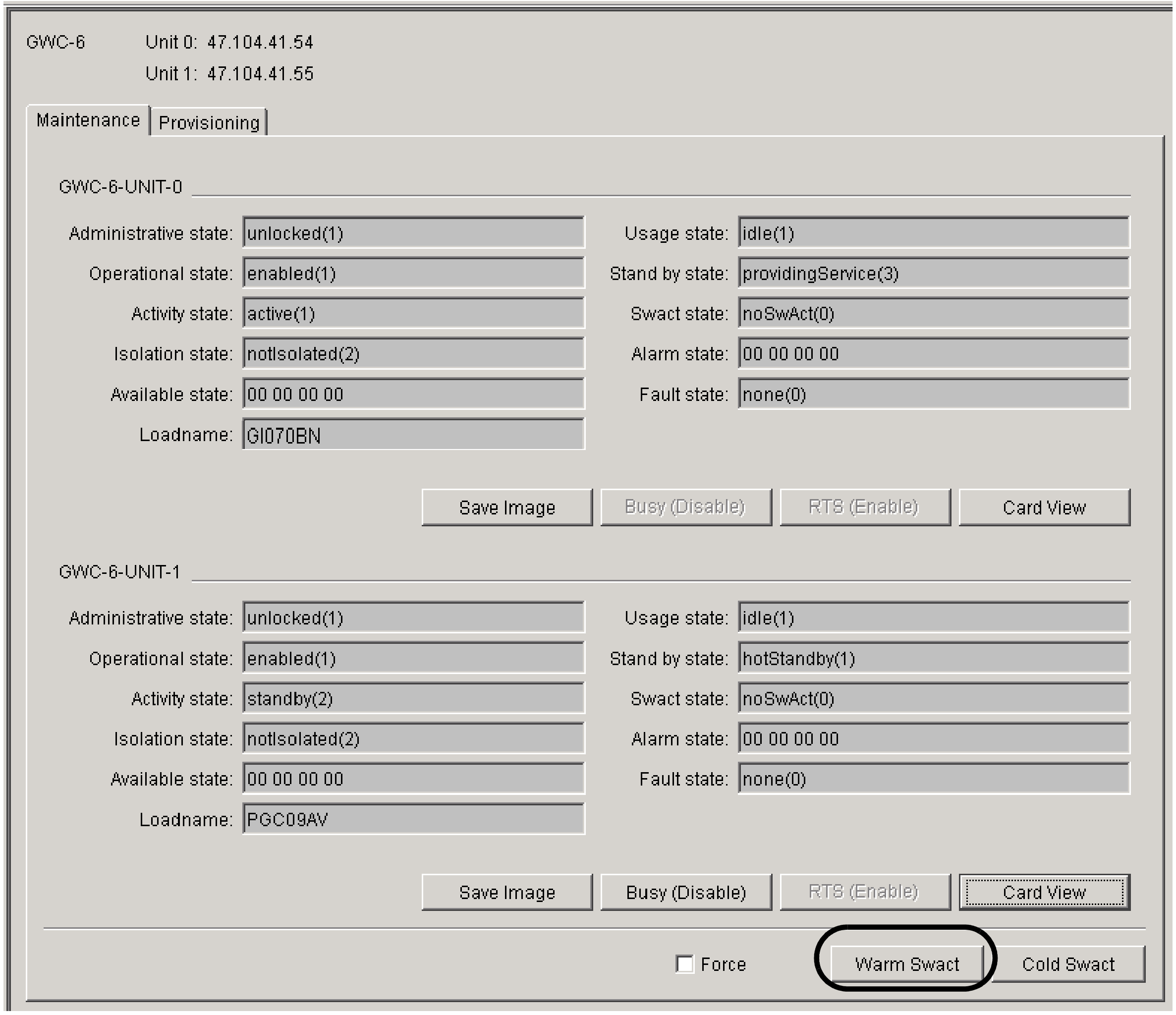
Administrative: Unlocked
Operational: Enabled
Availability: None

```
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

At the CS 2000 GWC Manager client

15 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”.

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



GWC-6 Unit 0: 47.104.41.54
Unit 1: 47.104.41.55

GWC-6-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	GI070BN		

GWC-6-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	noSwAct(0)
Isolation state:	notIsolated(2)	Alarm state:	00 00 00 00
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AV		

17 Return to step 3 and repeat the procedure for the mate GWC card in this node.

18 This procedure is complete.

Note: To return to the Overall GWC downgrade procedure, refer to Overall GWC downgrade procedure on page 7.

Reprovision Passport port to disable auto-negotiate

To disable auto-negotiation of the Ethernet port speed and duplex state, perform the following steps at the command line interface to the Passport router switch.

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

At the CLI for the Passport

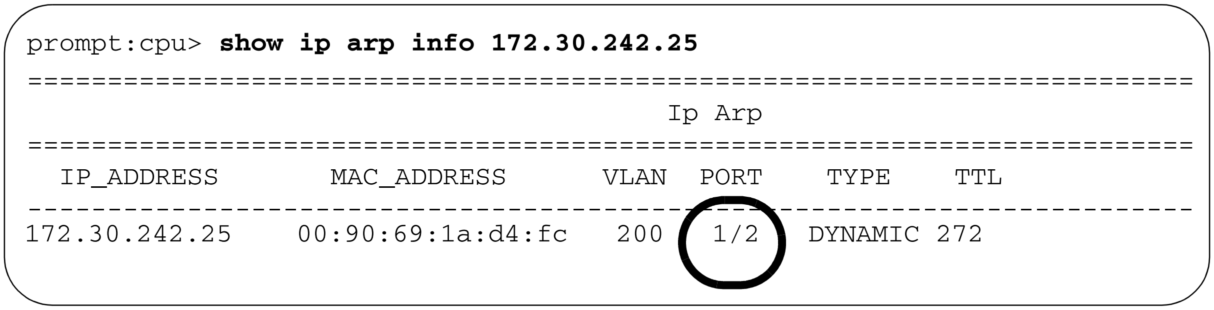
1 Determine the slot and port on the Passport that connects to the device by typing

> show ip arp info <ip_address>

and pressing the Enter key.

ip_address
is the physical IP address of the GWC card.

The slot and port are reported.



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

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

2 Disable auto-negotiation and reconfigure the slot and port by typing:

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

> config ethernet <slot>/<port> speed 100

> config ethernet <slot>/<port> duplex half

and pressing the Enter key.

The slot and port are reconfigured and the prompt returns.

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

3 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     false  false  half  100   half 100  fals  core  1   0
```

4 Commit the change by typing

> save config

and pressing the Enter key.

5 Go to step 8 to continue with the procedure “Rollback a software upgrade on a standby GWC”.

Launch CS 2000 Management Tools client applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- Succession SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same server as the CS 2000 Management Tools

  Note: The NPM also has a command line user interface (CLUI). Refer to procedure Access the Network Patch Manager CLUI on page 82 in this document.

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

- Launching applications from a web browser on page 71. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 74.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching applications from a desktop icon or Start menu (Windows only) on page 77.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching specific applications using a URL on page 80.

Note: You can also launch applications from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, NN10329-111.

Prerequisites

Ensure the client workstation meets the minimum requirements. Refer to section “Client workstation requirements” under “CS 2000 Management Tools” in the Basics document, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: http://developer.java.sun.com/developer/bugParade/bugs/4713003.html. A workaround for this issue is to download the latest ATI graphics driver from the following web site http://mirror.ati.com/support/driver.html. Contact your IT support team if you need assistance.

You need the IP address or host name of the server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

Note: Users of the CS 2000 Management Tools client applications must belong to the primary user group “succssn” for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure “Setting up local user accounts on a Sun server” in the ATM/IP Security and Administration document, NN10402-600.

You must have Java^{TM} 2 Runtime Environment (JRE) version 1.4.1_02 and Java^{TM} Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

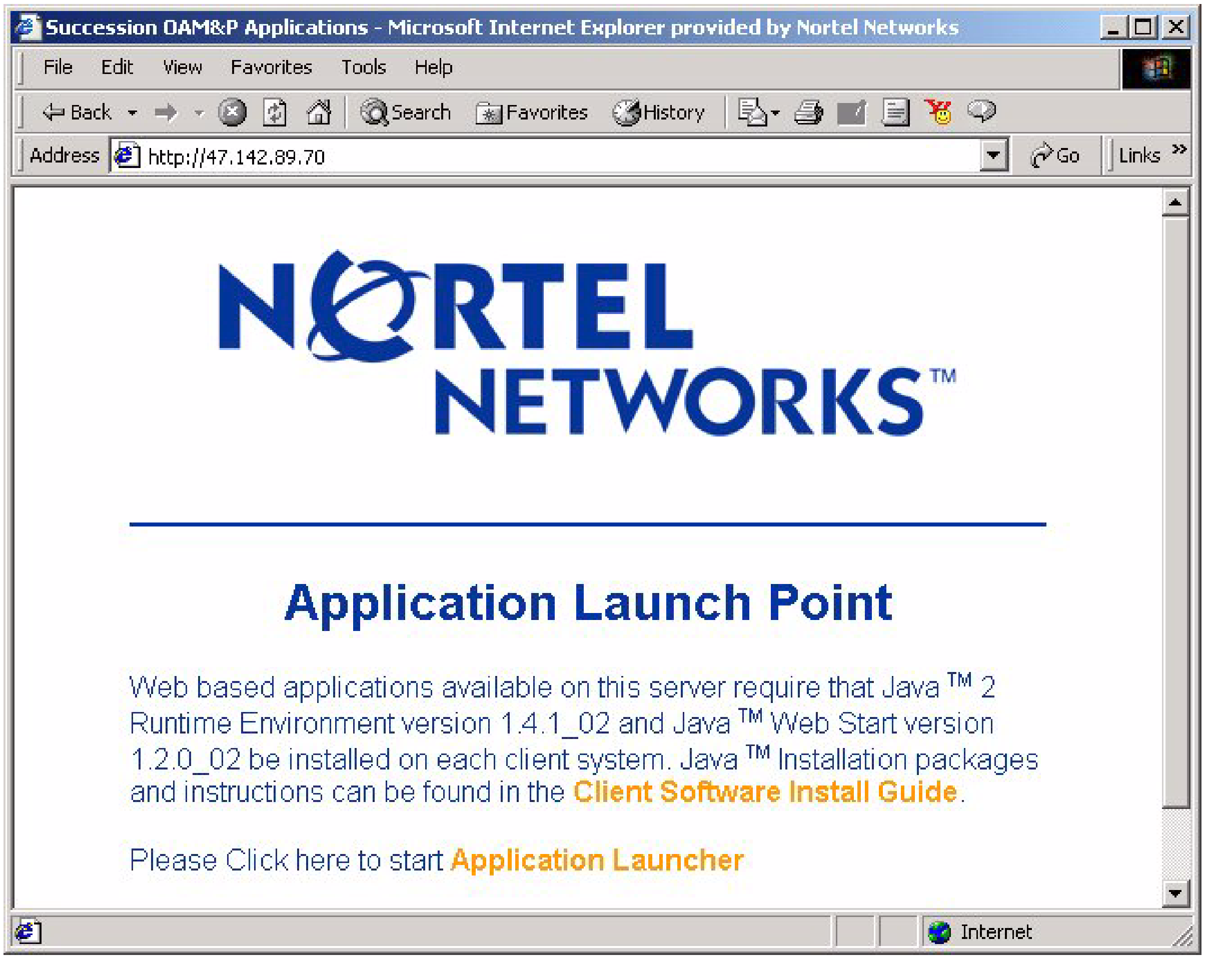
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

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

The “Application Launch Point” page appears.



Succession OAM&P Applications - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
http://47.142.89.70
Go
Links
NORTEL NETWORKS™
Internet

Application Launch Point

Web based applications available on this server require that Java ™ 2 Runtime Environment version 1.4.1_02 and Java ™ Web Start version 1.2.0_02 be installed on each client system. Java ™ Installation packages and instructions can be found in the Client Software Install Guide.

Please Click here to start Application Launcher

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

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

4 Click **Client Software Install Guide** and follow the instructions under “How to check version” to verify your client setup.

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

5 Click **Java 2 Runtime Environment Install Guide** under “Microsoft Windows” or “Sun Solaris” for system requirements and installation instructions.

6 Once you have read through the “Java 2 Runtime Environment Install Guide”, click the **Back** button to return to the “Client Software Installation” page.

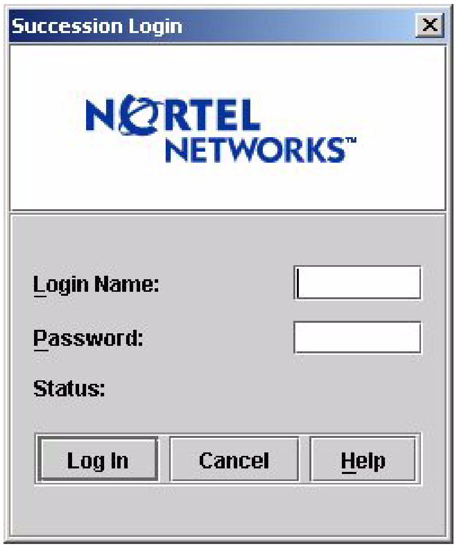
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

8 Click the **Back** button to return to the “Application Launch Point”.

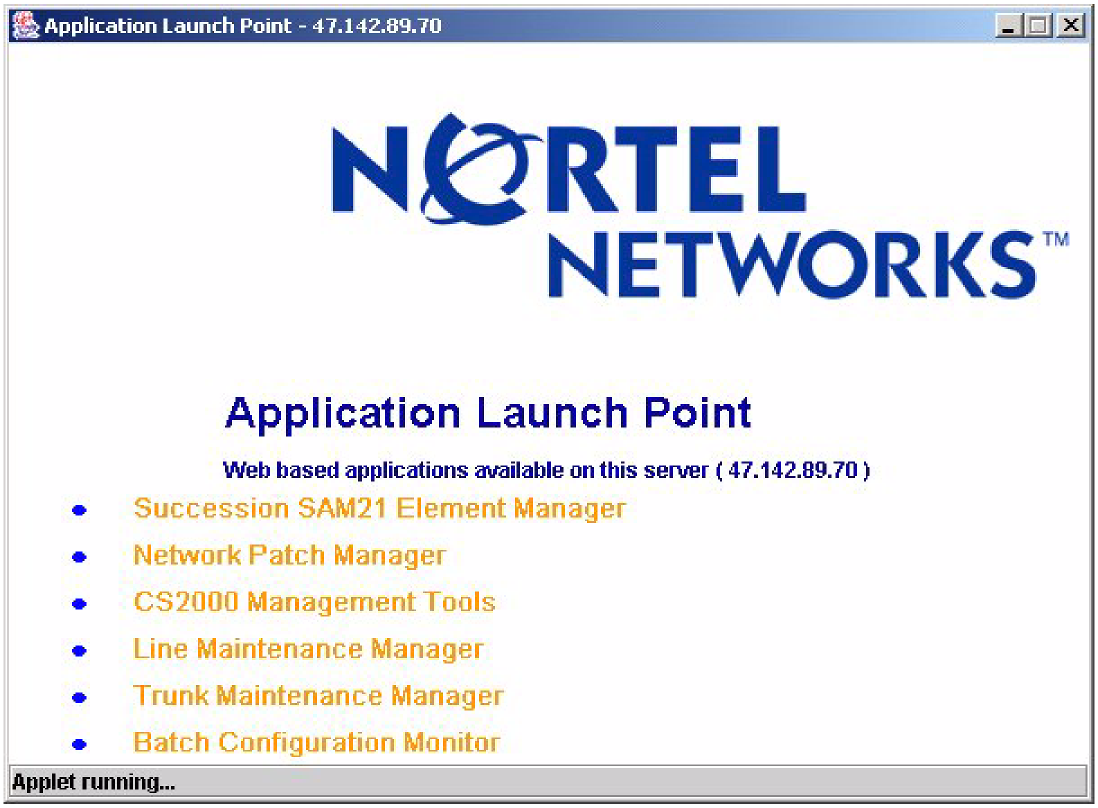
9 Click **Application Launcher**.

The Login window appears.



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

The Application Launch Point, similar to following, appears.


Application Launch Point - 47.142.89.70
NORTEL NETWORKS™
Application Launch Point
Web based applications available on this server (47.142.89.70)
Succession SAM21 Element Manager
Network Patch Manager
CS2000 Management Tools
Line Maintenance Manager
Trunk Maintenance Manager
Batch Configuration Monitor
Applet running...

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

The interface for the application you launched, is displayed.

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

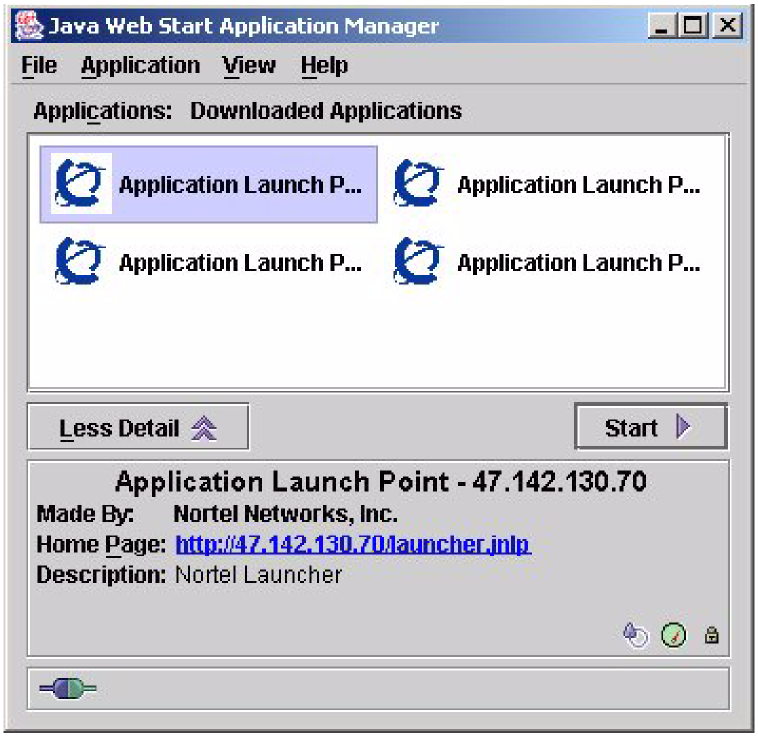
12 You have completed this procedure.

Launching applications from the JWS Application Manager

> **ATTENTION**
> You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Launch the Java Web Start Application Manager.



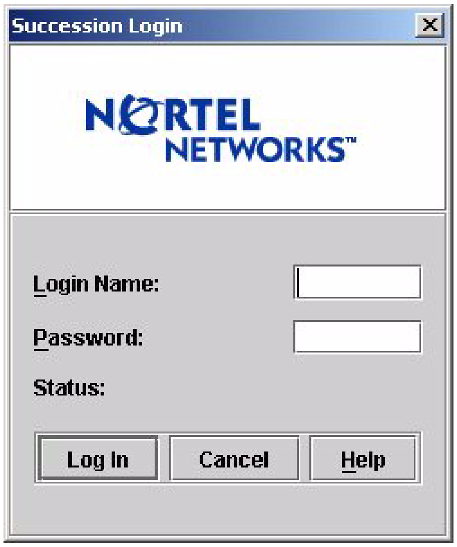
Application Launch Point - 47.142.130.70
Made By: Nortel Networks, Inc.
Home Page: http://47.142.130.70/launcher.jnlp
Description: Nortel Launcher

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

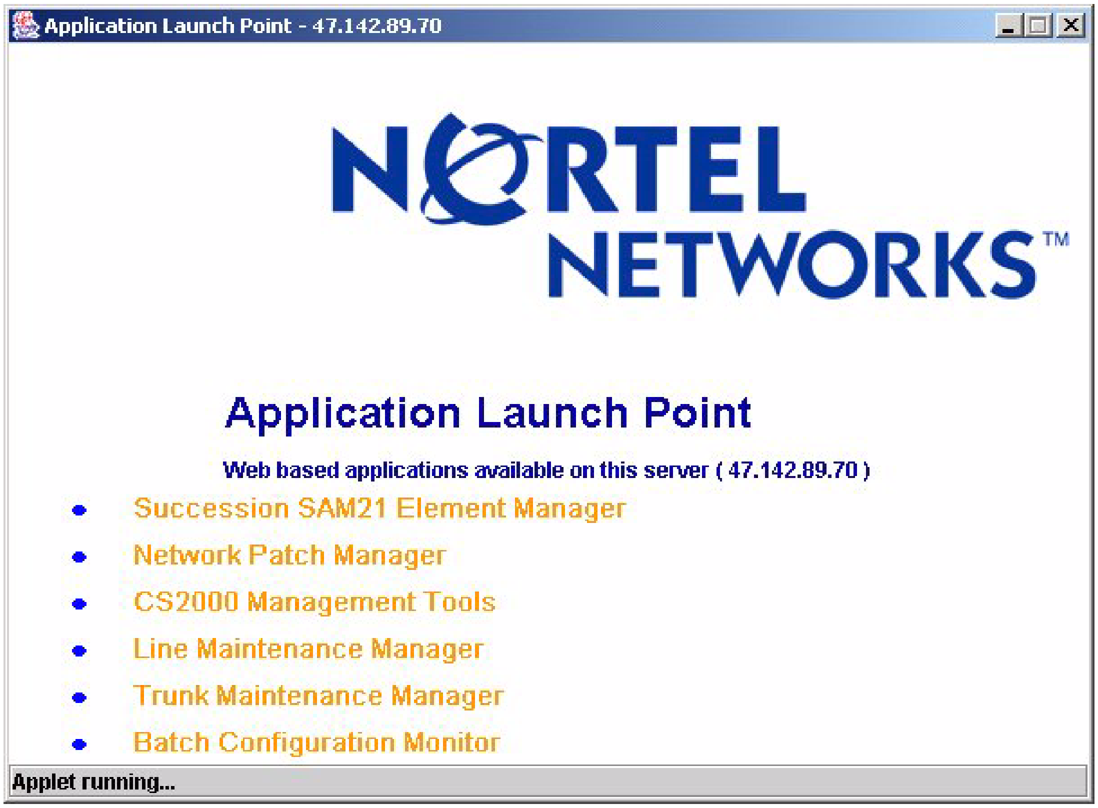
2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

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



The Application Launch Point, similar to following, appears.



Application Launch Point - 47.142.89.70

Application Launch Point

Web based applications available on this server (47.142.89.70)

- Succession SAM21 Element Manager
- Network Patch Manager
- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor

Applet running...

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

The interface for the application you launched, is displayed.

5 You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

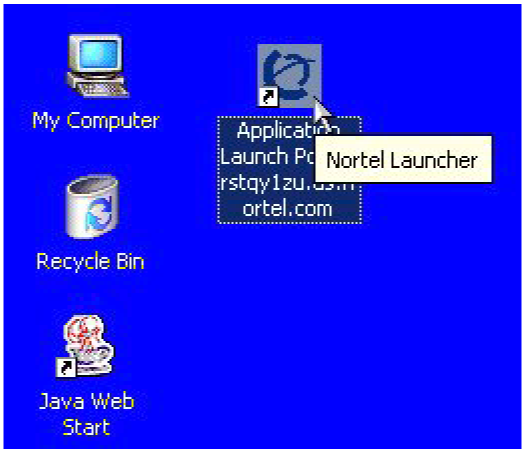
ATTENTION
You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

At your workstation

1 Perform step a to launch an application from a desktop icon, or b to launch an application from the Start menu.

a To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double click on it to start the application.

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

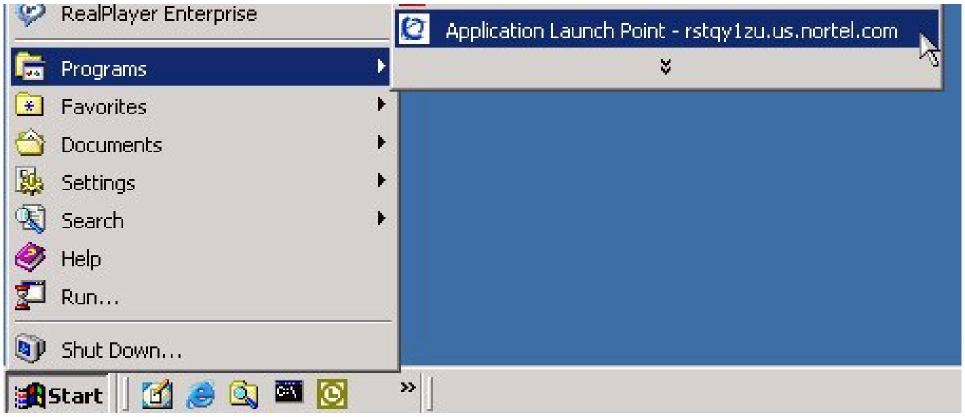


The Login window appears.

Proceed to step 2.

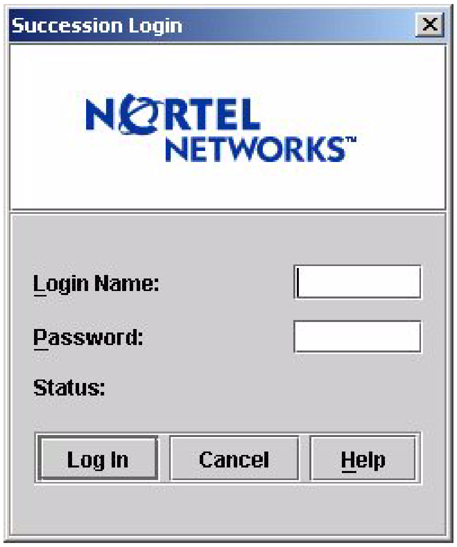
OR

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

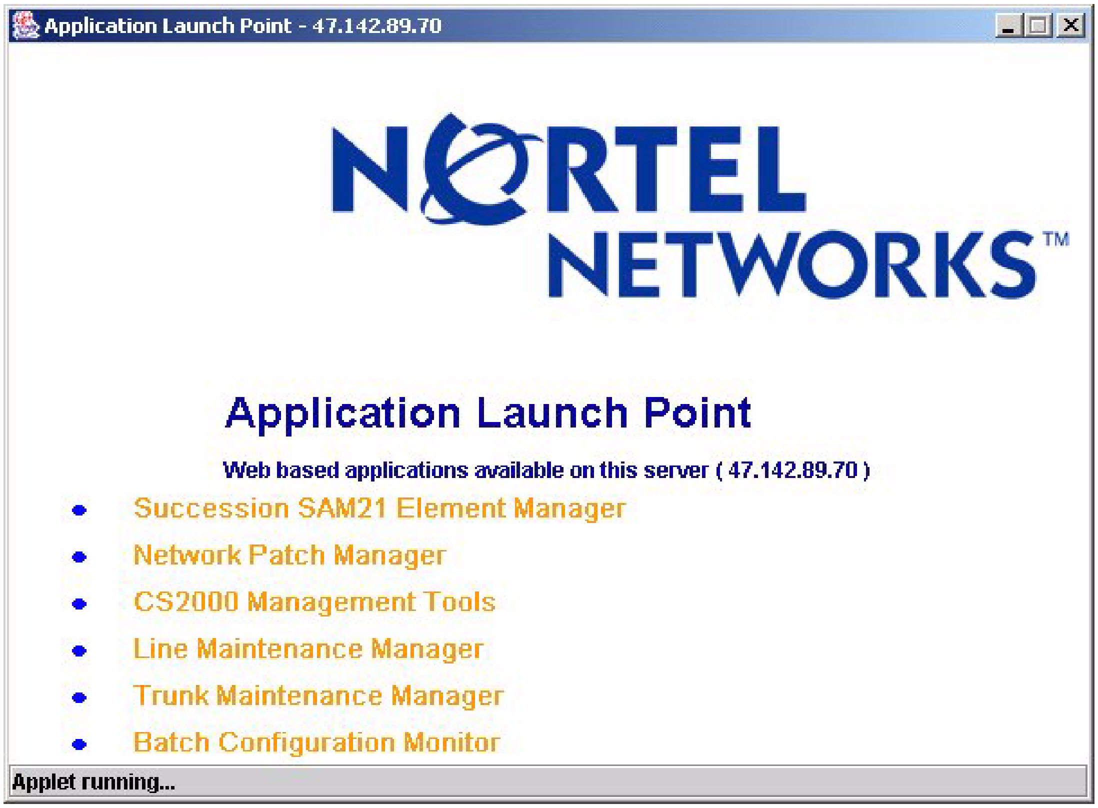


The Login window appears.

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



The Application Launch Point, similar to following, appears.



Application Launch Point - 47.142.89.70

NORTEL NETWORKS™

Application Launch Point

Web based applications available on this server (47.142.89.70)

- Succession SAM21 Element Manager
- Network Patch Manager
- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor

Applet running...

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

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java^{TM} 2 Runtime Environment (JRE) version 1.4.1_02 and Java^{TM} Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser on page 71.

At your workstation

1 Launch your web browser.

2 In the Address field, enter one of the following URLs for the application you want to launch:

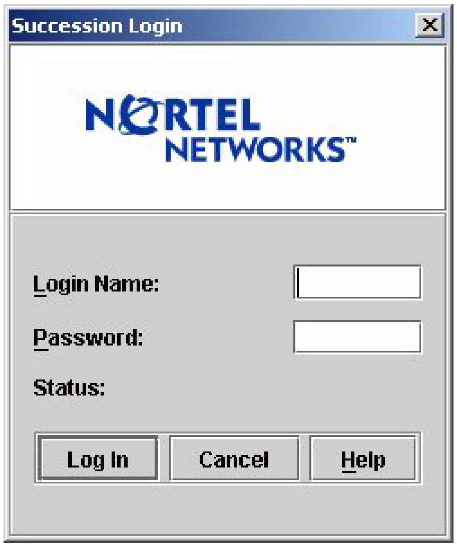
Application	URL
CS2000 Management Tools	http://<host>/:8080/launch/servlet/Launch?app=sesm
Line Maintenance Manager	http://<host>/:8080/launch/servlet/Launch?app=lmm
Trunk Maintenance Manager	http://<host>/sesm/tmm.html
Batch Configuration Monitor	http://<host>/sesm/bpt.html
CS2000 SAM21 Manager	http://<host>/:8080/launch/servlet/Launch?app=sam21em
Network Patch Manager	http://<host>/:8080/launch/servlet/Launch?app=npm

Where

host
is the host name or IP address of the server where the application resides

The Login window appears.

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



The interface for the application you launched, is displayed.

4 You have completed this procedure.

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and Succession SAM21 Element Manager) connect to their corresponding server-side application through a Socks proxy.

> ***Note:*** The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

If, when you launch a client application that connects through a Socks proxy, you receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can re-launch the client application.

Access the Network Patch Manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

> ***Note 1:*** You can also access the NPM CLUI from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, NN10329-111.
>
> ***Note 2:*** The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launch CS 2000 Management Tools client applications on page 69 in this document.

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter ‘npm’ commands, help
or quit to exit.

npm>
```

5 You have completed this procedure.

Perform a device audit using the NPM

Application

Use this procedure to perform a device audit using the Network Patch Manager (NPM). You can perform a device audit using one of the following two NPM interfaces:

- Using the NPM CLUI on page 84
- Using the NPM GUI on page 85

It is recommended that you perform an audit on devices prior to patching.

An audit determines whether the NPM database has accurate device patch information. If the patch category or patch status fields are blank for any patches, complete procedure Transfer patches to the NPM database manually on page 89 if required.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1. Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 if required.

At the NPM CLUI

2 Audit the device by typing

```
npm> auditd <devices>
```

and pressing the Enter key.

where

devices
is a list of one or more device IDs for which you want to run the audit - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example
`npm> auditd` GWC-8-UNIT-1

3 You have completed this procedure.

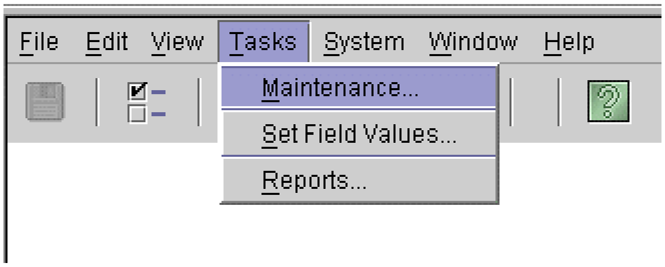
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 if required.

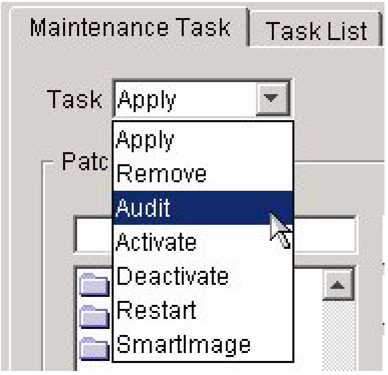
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.



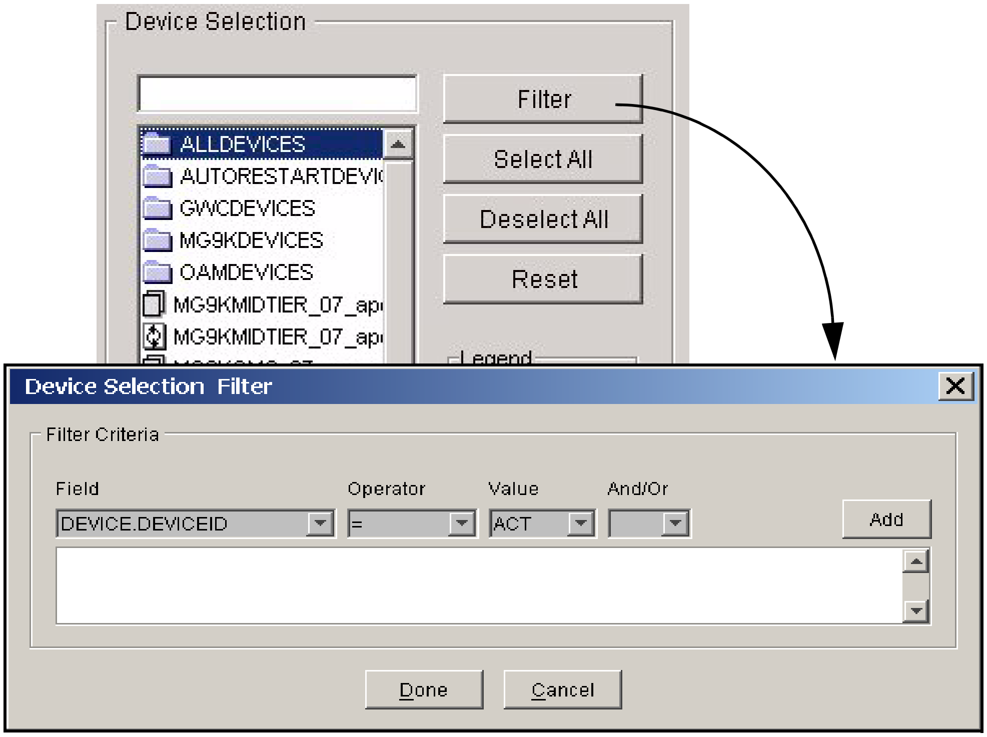
The Maintenance window is displayed.

3 In the **Task** list, click **Audit**.



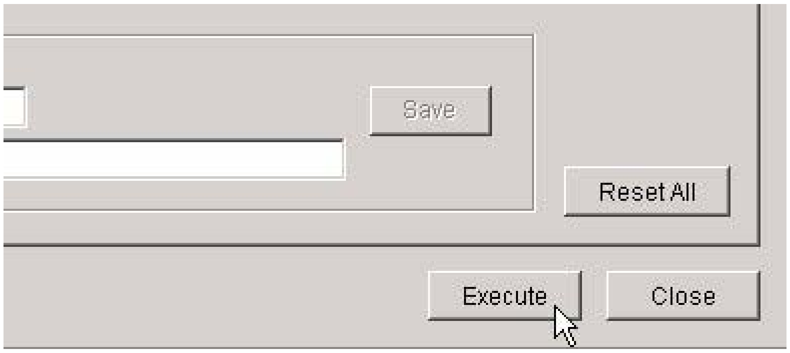
Task: Apply

4 In the **Device Selection** list, select the devices or device sets you want to audit, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.

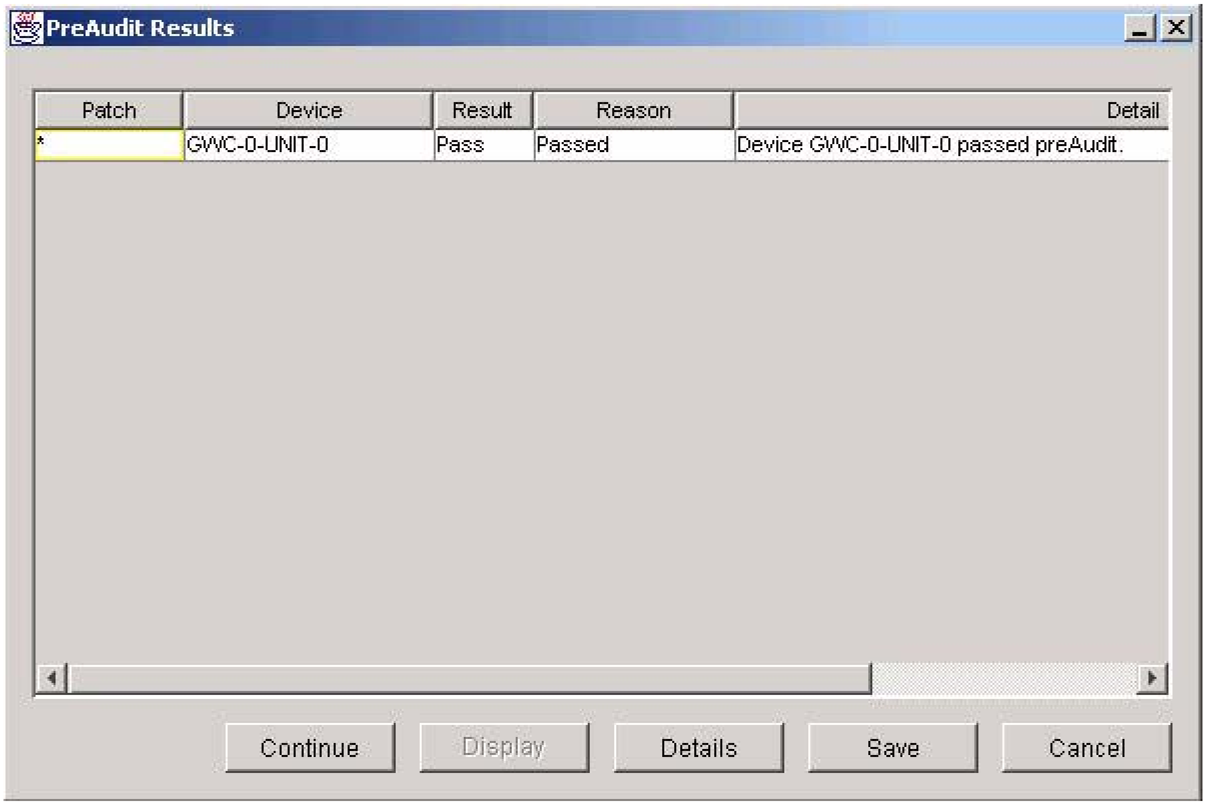


Field	Operator	Value	And/Or
DEVICE.DEVICEID	=	ACT	

5 Click the **Execute** button to begin the audit process.



The results of the PreAudit phase are displayed.

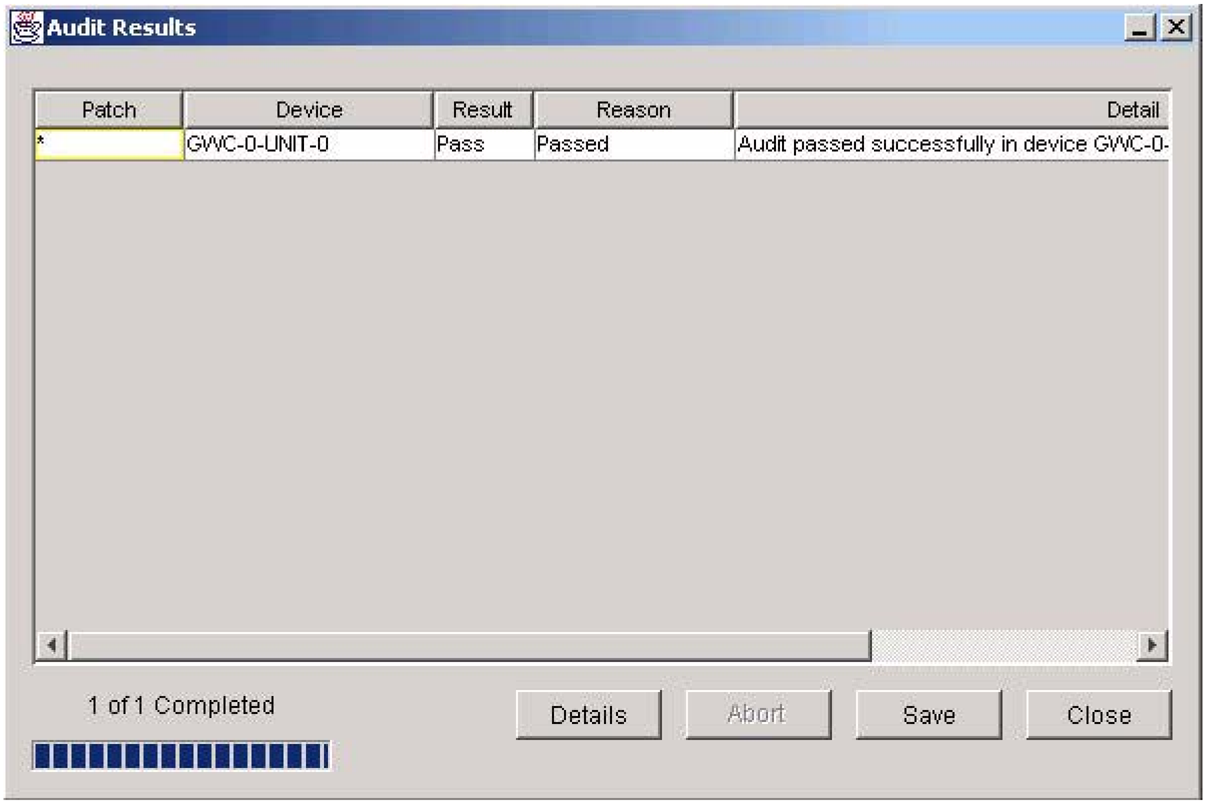


Patch	Device	Result	Reason	Detail
*	GWC-0-UNIT-0	Pass	Passed	Device GWC-0-UNIT-0 passed preAudit.

6 Review the PreAudit Results, then click **Continue** to proceed.

Note: The Patch field in the Results Table will indicate an asterisk (*) for each operation since only the device is related to the operation.

The Audit Results window is displayed with results added as each action is completed. Failures from the PreAudit phase are also included in the results.



Patch	Device	Result	Reason	Detail
*	GWC-0-UNIT-0	Pass	Passed	Audit passed successfully in device GWC-0-

7 Click **Save** to save the results to a file, or click **Close**.

Note: If the audit does not successfully complete, abort the audit procedure and contact your next level of support.

8 You have completed this procedure.

Transfer patches to the NPM database manually

Application

Use this procedure to manually transfer patches to the Network Patch Manager (NPM) database and retrieve them for processing. Patches can be delivered either on a CD or electronically.

> ***Note:*** You can enable automatic patch file delivery to the NPM database, including patch retrieval for processing, by enabling the Patch File Receipt System (PFRS). Refer to procedure “Configuring NPM for automatic patch file delivery” in the ATM/IP Solution-level Configuration Management document, NN10409-500, to enable PFRS or determine if it is already enabled.

Also use this procedure when you are attempting to audit or apply patches that have a blank patch category or patch status field.

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

ATTENTION
In a two-server configuration, perform this procedure on the Active server.

At the Sun server

1 Use the following table to determine how to proceed.

If patches were delivered	Do
on CD	step 2
electronically	step 3

2 Insert the CD that contains the patches into the CD drive of the Sun server where NPM resides.

At your workstation

3 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server where NPM resides

4 When prompted, enter your user ID and password.

5 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If patches were delivered	Do
on CD	step 8
electronically	step 13

8 Make a temporary directory for the patchlist file by typing

```
# mkdir /data/npm/tmp
```

and pressing the Enter key.

9 Change the permissions on the temporary directory by typing

```
# chmod 777 /data/npm/tmp
```

and pressing the Enter key.

10 Create the ".patchlist" file for all the patches that are on the CD, in the temporary directory by typing

```
# find /cdrom -name "*.patch" >
/data/npm/tmp/current.patchlist
```

and pressing the Enter key.

11 Access the directory you just created by typing

```
# cd /data/npm/tmp
```

and pressing the Enter key.

12 Proceed to step 23.

13 Make a directory for the patch files you want to install by typing

```
# mkdir /data/npm/patch_upgrade
```

and pressing the Enter key.

14 Change the permissions on the newly created directory by typing

```
# chmod 777 /data/npm/patch_upgrade
```

and pressing the Enter key.

15 Access the newly created directory by typing

```
# cd /data/npm/patch_upgrade
```

and pressing the Enter key.

16 FTP to the ESD server by typing

```
# ftp <ESD_server>
```

and pressing the Enter key.

where

ESD_server
is the IP address of the ESD server

17 When prompted, enter your user ID and password for the ESD server.

18 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

19 Transfer all the patches from the ESD server to the NPM by typing

```
ftp> mget *.patch
```

and pressing the Enter key.

Note: To transfer individual patch files, enter the following command:

```
ftp> get <patch_filename>
```

20 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

21 Verify the patches are in the temporary directory on the Sun server by typing

```
# ls
```

and pressing the Enter key.

22 Change permissions for the patch files in the directory by typing

```
# chmod 777 *
```

and pressing the Enter key.

23 Verify the NPM server application is running by typing

```
# servquery -status -group NPM
```

and pressing the Enter key.

If the NPM server application is	Do
not running	step 24
running	step 25

24 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

25 Access the NPM command line user interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

26 When prompted, enter your user ID and password.

Note: Do not change directory.

27 Retrieve the patch files for the NPM to process as follows

If	Type
You want to retrieve the patch files copied from the CD	npm> **getpatch current.patchlist**
You want to retrieve the patch files copied from the electronic service delivery system (ESD)	npm> **getpatch <patch_filename>**

and press the Enter key.

where

patch_filename
is either the name of the file that contains names of the patch files to retrieve (must end with ".patchlist"), or an actual patch file

28 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

29 Change directory by typing

```
# cd
```

and pressing the Enter key.

Note: You must change directory from the cdrom directory using the "cd" command for the "eject cdrom" command to execute successfully.

30 Eject the CD from the drive by typing

```
# eject cdrom
```

and pressing the Enter key.

If you have	Do
other patch CDs	insert the next CD and go to step 10
no other patch CDs	close the cdrom tray

31 You have completed this procedure.

Define reports using the NPM

Application

Use this procedure to create a user-defined report and generate it using the Network Patch Manager (NPM). You can define reports using one of the following two NPM interfaces:

- Using the NPM CLUI on page 95
- Using the NPM GUI on page 96

The reporting feature of the Network Patch Manager (NPM) allows you to select information from the database and display it. Report criteria determines what is displayed. In addition to the predefined reports for the NPM, users can create and save their own reports according to their application-specific criteria.

The NPM is initially configured with the following defined reports:

- ACTLIST - RPS activation patch information
- CALCLIST - RPS patch calculation report
- DEVICE - Information about a specific device (prompt report)
- DEVICELIST - Information about patchable devices on the system
- DISABLEDAPPLIED - patches that are applied but disabled
- DISABLEDREMOVED -patches that are disabled and removed
- ENABLEDAPPLIED - patches that are applied and enabled
- ENABLEDREMOVED - patches that are applied but removed
- FULLDEVICELIST - Information about every device on the system
- LOADLIST - RPS device load report
- PATCH - Information about a specific patch (prompt report)
- PATCHES_SINCE - Patch activity since a specific date (prompt report)
- PATCHINFO - Full information about a specific patch (prompt report)
- PATCHLIST - Information about patches and their relationships on the system
- DEVICE_ACTIVITY -Displays all devices and their activity states
- DEVICE_ACTLEVEL - Displays the number of patches activated in each device

- DEVICE_APPLEVEL - Displays the number of patches applied to each device
- INVALID_LOADNAME - Displays devices with invalid loads. An audit is required (see procedure Perform a device audit using the NPM on page 84 in this document if required).

Prerequisites

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 in this document, if required.

At the NPM CLUI

1 Define the report by typing

```
npm> newset REPORT <report_name> <report_desc>
<report_fields> where <report_criteria>
```

and pressing the Enter key.

where

report_name
the name of the report to be created

report_desc
is a short description of the report

report_fields
is the name of one or more fields, separated by a space, to be included in the report

report_criteria
is the SQL statement that identifies the criteria by which to search the NPM database

Example

```
npm> newset REPORT DEVHOLDFALSE “All devices
with HOLD=FALSE” “DEVICE.DEVICEID DEVICE.HOLD
where DEVICE.HOLD=’FALSE’”
```

2 Generate the report by typing

```
npm> query <report_name>
```

and pressing the Enter key.

where

report_name
the name of the report you previously created

3 You have completed this procedure.

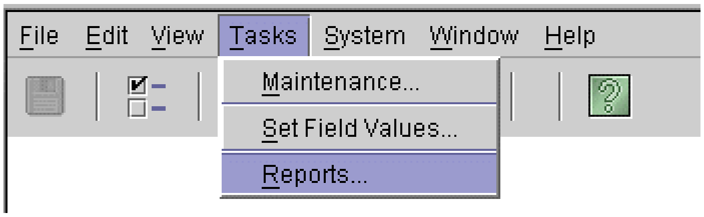
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 in this document, if required.

At the NPM GUI

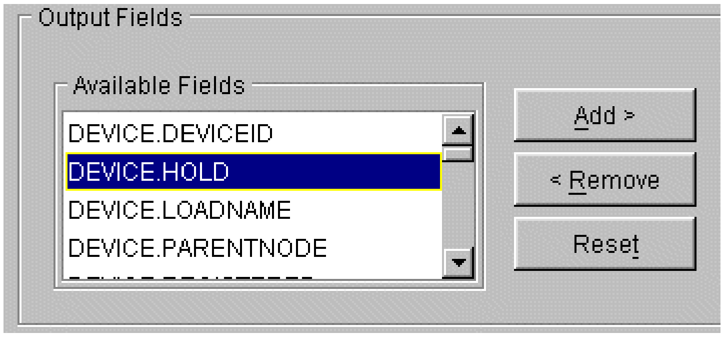
1 On the **Tasks** menu, click **Reports...**.



2 Specify the fields to be included in the new report as follows:

Note: You can also edit an existing report listed under the **Report List** tab, that contains similar criteria to the report you want to create, and save it under a new name.

a In the **Available Fields** list, click a field of your choice.



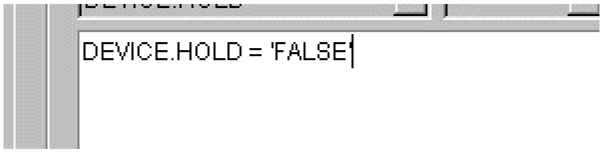
b Click **Add** to add the field to the **Selected Fields** list.

c Repeat Steps 2a and 2b for each field, then proceed to step 3.

3 In the **Report Criteria** area, specify the criteria for the report using substep a or b

a Type the criteria for the report in the text box.

Note: Parenthesis “()” may be inserted to define precedence for multiple criteria statements.

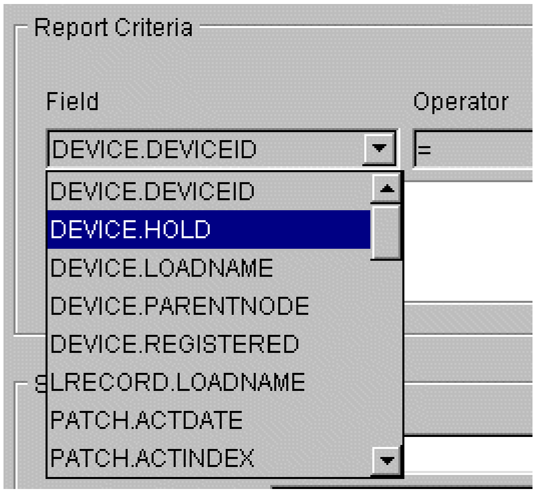


DEVICE.HOLD = 'FALSE'

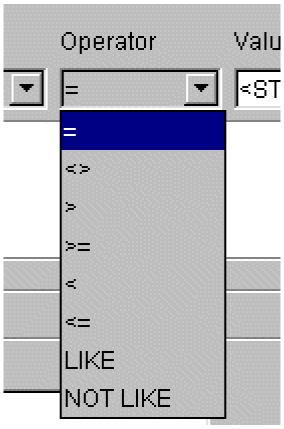
OR

b Specify the report criteria as follows:

i In the **Field** list, click the field of your choice.



ii In the **Operator** list, click the operator of your choice.



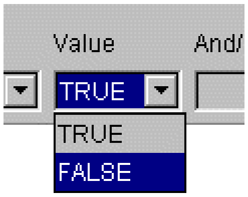
The table below lists the supported operators and their meaning.

Operator	Meaning
=	Equal
<>	Not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal

Operator	Meaning
LIKE	Matches string with wildcard (%)
NOT LIKE	Does not match string with wildcard (%)

iii In the **Value** list, select the value of your choice

Note: The data type in the **Value** list will change depending on the data type selected in the **Field** list. For alphanumeric data, type the value. For boolean data, select the value.

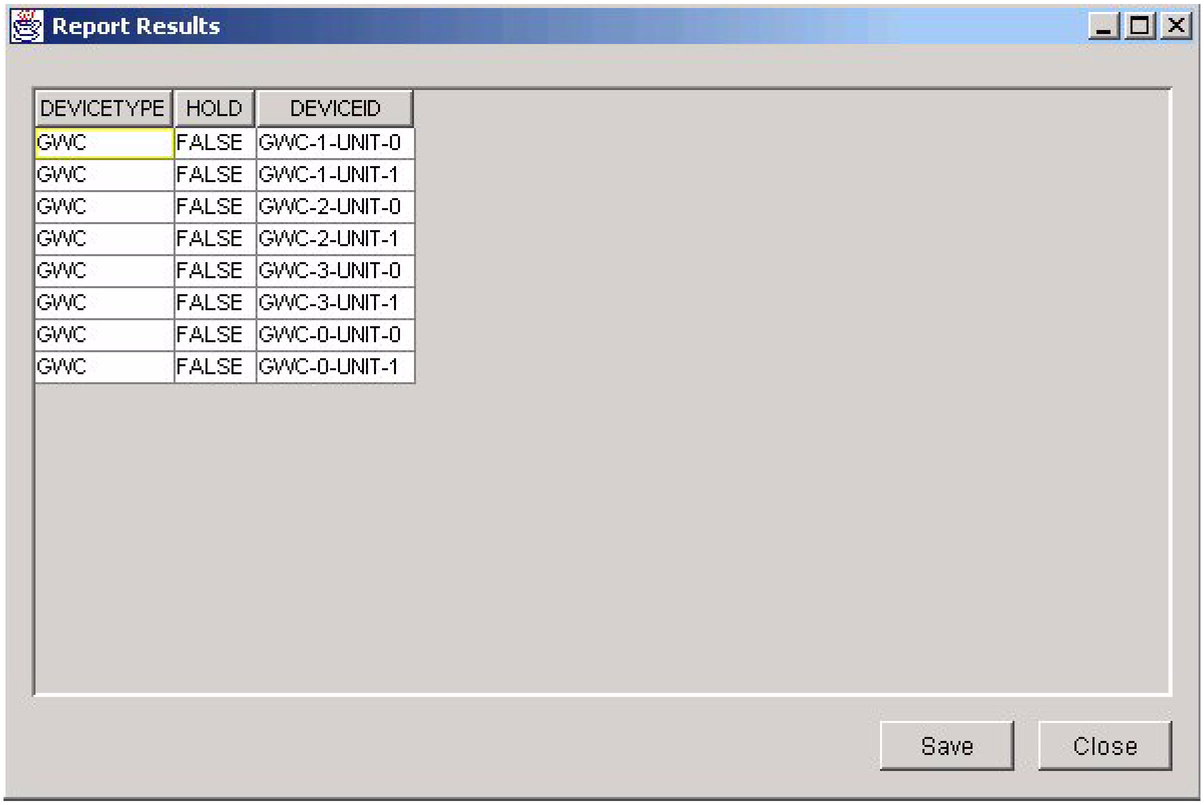


To combine multiple criteria statements, click **AND** or **OR** in the **And/Or** list.

4 Click **Execute** to generate the report.

The system displays the Report Results window.

> ***Note:*** The time required to generate the report depends on the number of patches and devices in the database and the complexity of the search criteria.



DEVICETYPE	HOLD	DEVICEID
GWC	FALSE	GWC-1-UNIT-0
GWC	FALSE	GWC-1-UNIT-1
GWC	FALSE	GWC-2-UNIT-0
GWC	FALSE	GWC-2-UNIT-1
GWC	FALSE	GWC-3-UNIT-0
GWC	FALSE	GWC-3-UNIT-1
GWC	FALSE	GWC-0-UNIT-0
GWC	FALSE	GWC-0-UNIT-1

5 You have completed this procedure.

Apply patches using the NPM

Application

Use this procedure to apply patches using the Network Patch Manager (NPM). You can apply patches using one of the following two NPM interfaces:

- Using the NPM CLUI
- Using the NPM GUI

Prerequisites

The patches must have already been transferred to the NPM database. Contact your network administrator to determine if this has already been done. If required, refer to procedure Transfer patches to the NPM database manually on page 89 to transfer the patches to the NPM database.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up users on a Sun server” in the ATM/IP Administration and Security document, NN10402-600.

It is recommended that you perform an audit on the devices prior to patching. Refer to procedure Perform a device audit using the NPM on page 84 if required.

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 if required.

At the NPM CLUI

2 Apply one or more patches to one or more devices by typing

```
npm> apply <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to apply - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices
is a list of one or more device IDs to which you want to apply the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and applies them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Note: Enclose the <deviceid> for GWC devices in single quotes (‘).

Example

```
npm> apply ACT02GAX in ‘gwc3 Unit 1 47.142.108.39’
```

3 When prompted, press the Enter key.

4 Generate a device query report to verify the patches are applied by typing

```
npm> q device
```

5 Enter the device name in the format **‘<deviceid>’** that you input in step 2.

Note: The GWC <device id> must be enclosed in single quotes (‘) only when the GWC device id has spaces, dashes or periods as part of its name.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are applied (status =A).

> ***Note:*** If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

If you applied patches to any of the following devices, you need to restart the device in order to enable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure “Restarting a device using the NPM” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

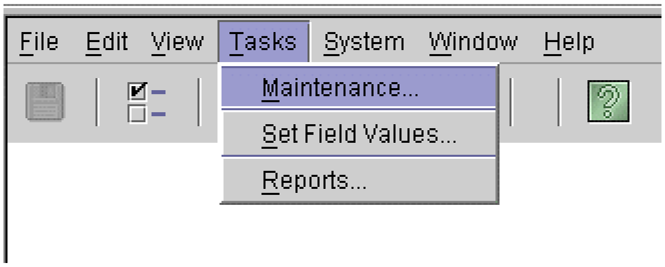
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 if required.

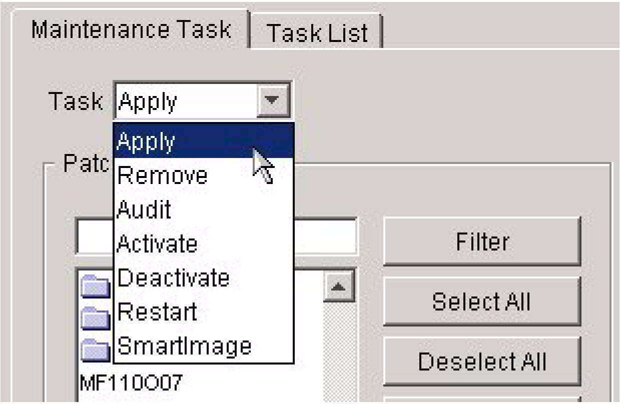
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

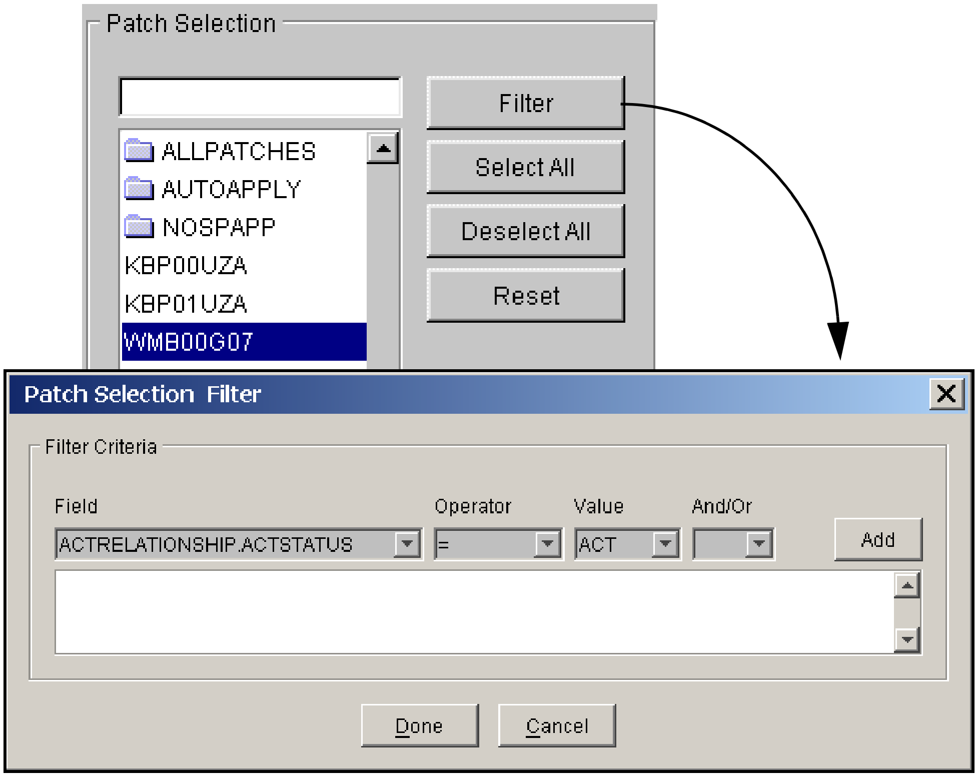


The Maintenance window is displayed.

3 In the **Task** list, click **Apply**.



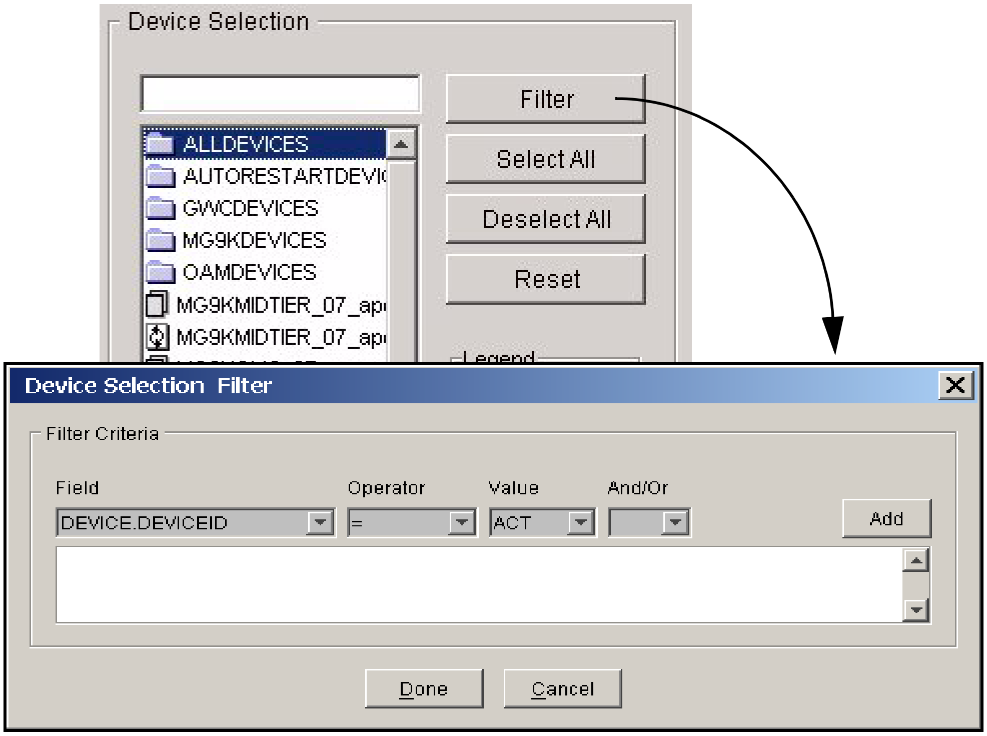
4 In the **Patch Selection** list, select the patch files or patch sets you want to apply, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



ALLPATCHES
AUTOAPPLY
NOSPAPP
KBP00UZA
KBP01UZA
WMB00G07

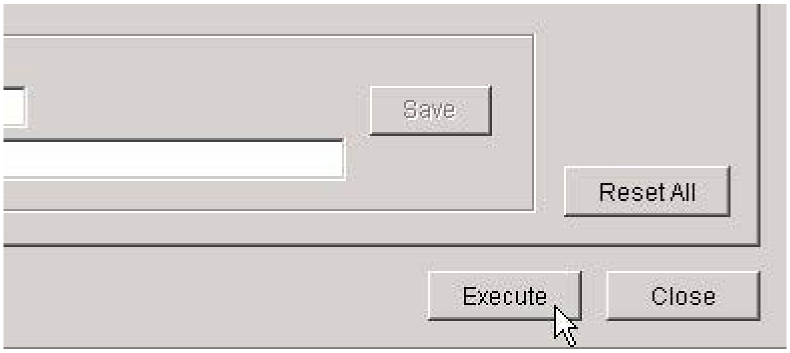
Field: ACTRELATIONSHIP.ACTSTATUS
Operator: =
Value: ACT
And/Or:

5 In the **Device Selection** list, select the devices or device sets to which you want to apply the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.

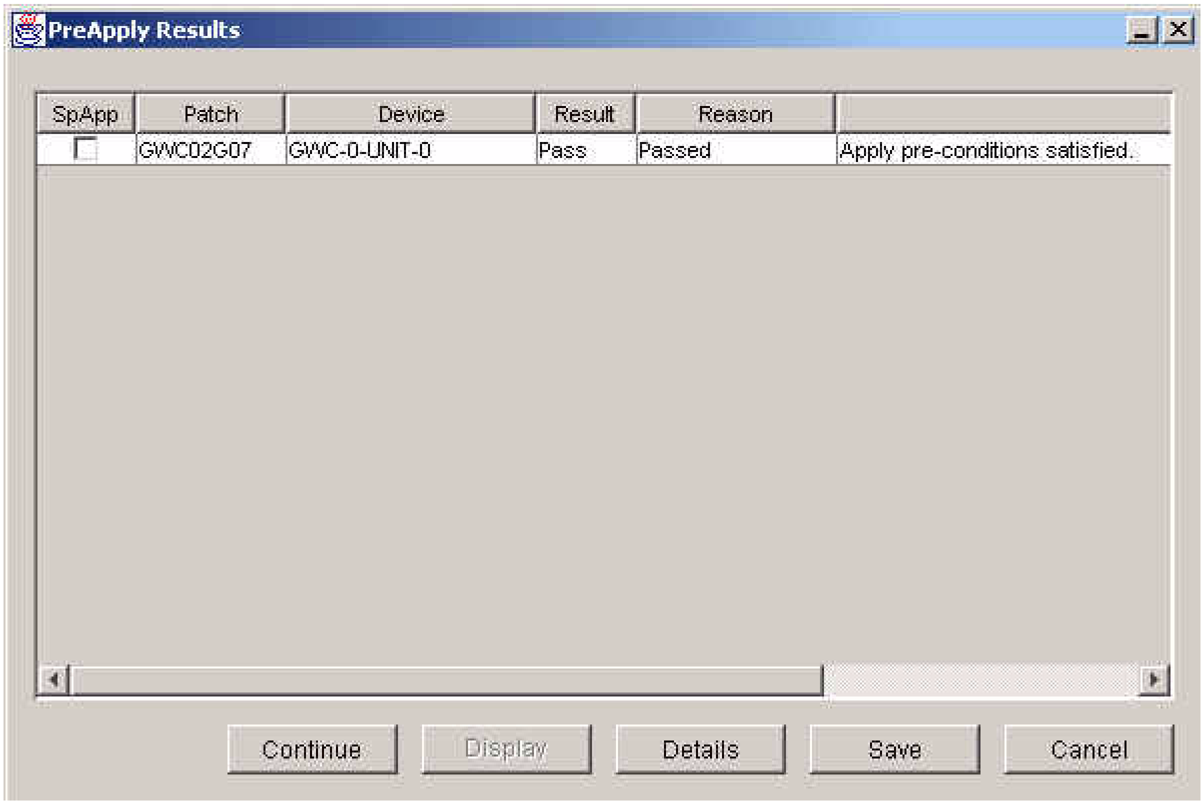


Field: DEVICE.DEVICEID
Operator: =
Value: ACT
And/Or:

6 Click **Execute** to begin the patching process.



The results of the PreApply phase are displayed.

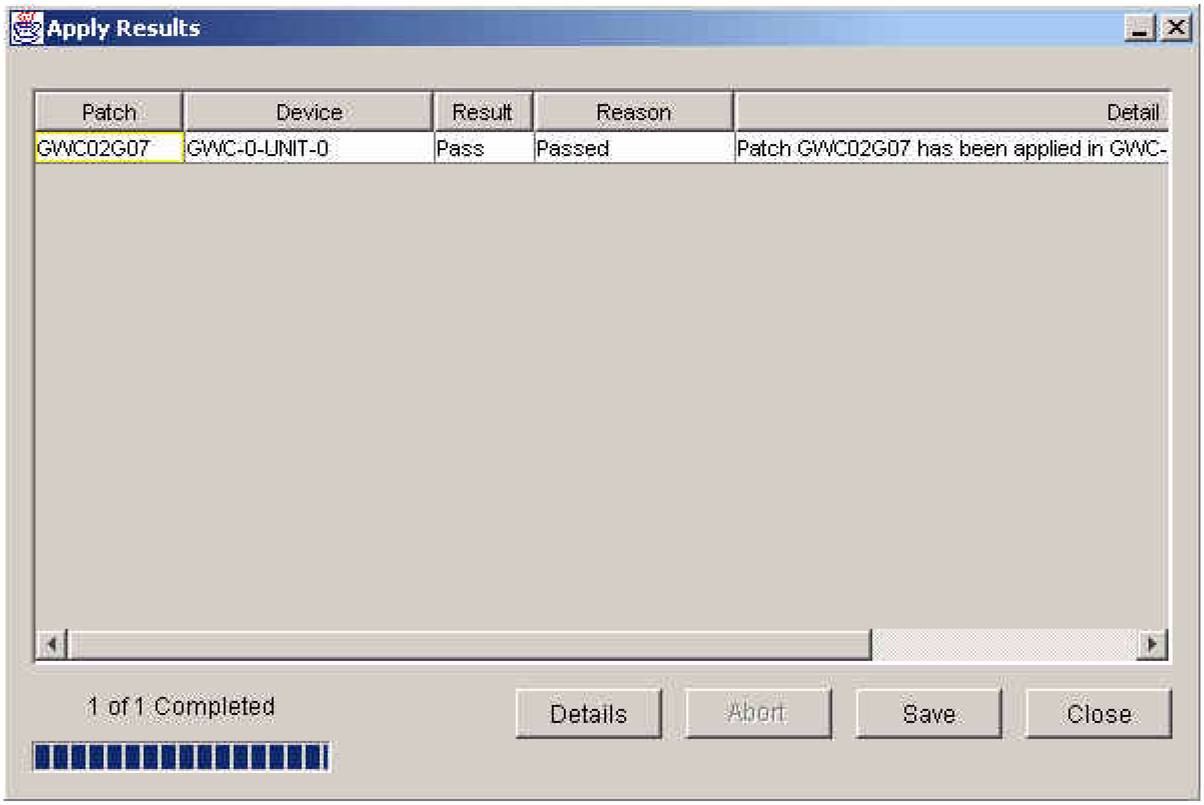


SpApp	Patch	Device	Result	Reason	
□	GWC02G07	GWC-0-UNIT-0	Pass	Passed	Apply pre-conditions satisfied.

7 Review the PreApply Results, then click **Continue** to proceed.

Note: If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Apply Results window is displayed with results added as each action is completed. Failures from the PreApply phase are also included in the results.



Patch	Device	Result	Reason	Detail
GWC02G07	GWC-0-UNIT-0	Pass	Passed	Patch GWC02G07 has been applied in GWC-

1 of 1 Completed

8 Click **Save** to save the results to a file, or click **Close**.

Note: If the patches do not successfully apply, abort the patching procedure and contact your next level of support.

9 You have completed this procedure.

If you applied patches to any of the following devices, you need to restart the device in order to enable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure “Restarting a device using the NPM” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Activate patches using the NPM

Application

Use this procedure to activate patches, which are deemed activatable by the ACT category, using the Network Patch Manager (NPM). You can activate patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 111
- Using the NPM GUI on page 112

Note: Currently, only GWC can have ACT category patches.

ATTENTION

Certain GWC patches may be ACT category patches that may require activation. It is important to note that not all ACT category patches require activating. The patches to be activated would depend on the requirements for the GWC load. Prior to activating the ACT category patches, it is important that you read and understand the administration section of the patch and make sure the ACT patch enables the functionality you require. If you are unsure about the impact of activating an ACT patch in your office, contact your next level of support to determine if the patches can be activated.

Prerequisites

You can activate a patch if all of the following criteria have been fulfilled:

- the patch has been identified by your support team and Nortel as being applicable and necessary for your site
- the patch is not on hold
- the patch has a category of ACT
- the patch has been applied

CAUTION

Do not activate patches for your components that have not been identified as needing activation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 in this document, if required.

At the NPM CLUI

2 Query the NPM for a list of patches that can be activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

3 Activate one or more patches for one or more devices by typing

```
npm> activate <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to activate - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices

is a list of one or more device IDs for which you want to activate the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and activates them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example

```
npm> activate ACT02GAX in GWC-8-UNIT-1
```

4 When prompted, press the Enter key.

5 Query the NPM to verify the patches are activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

6 Verify from the list that the desired patches are activated.

> ***Note:*** If the patches do not successfully activate, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

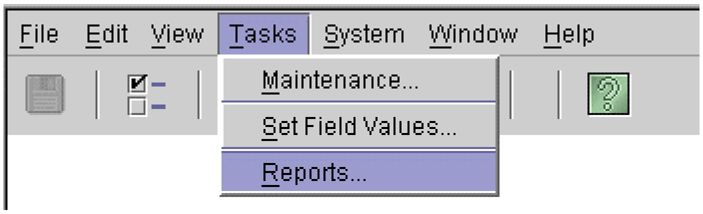
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 in this document, if required.

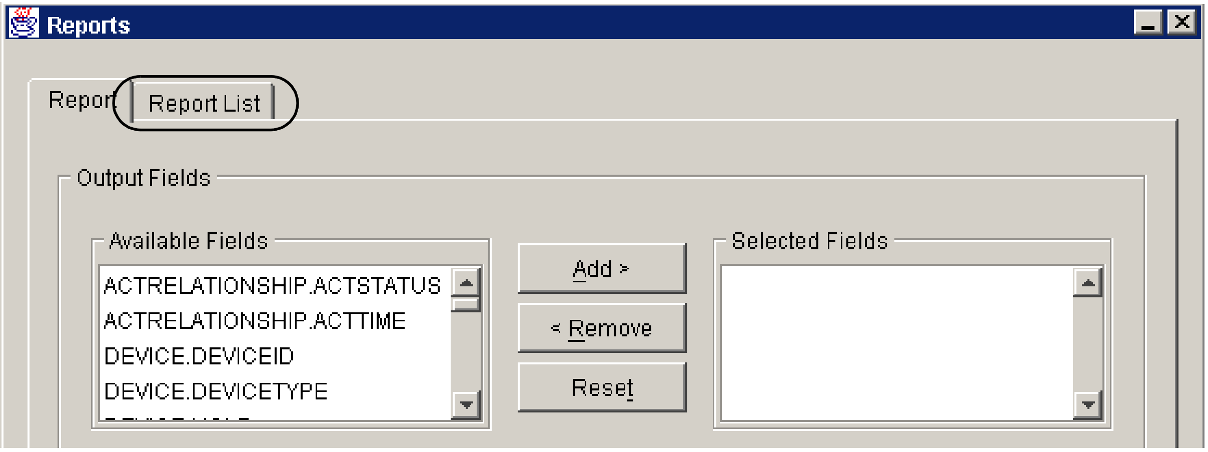
At the NPM GUI

2 On the **Tasks** menu, click **Reports...**.

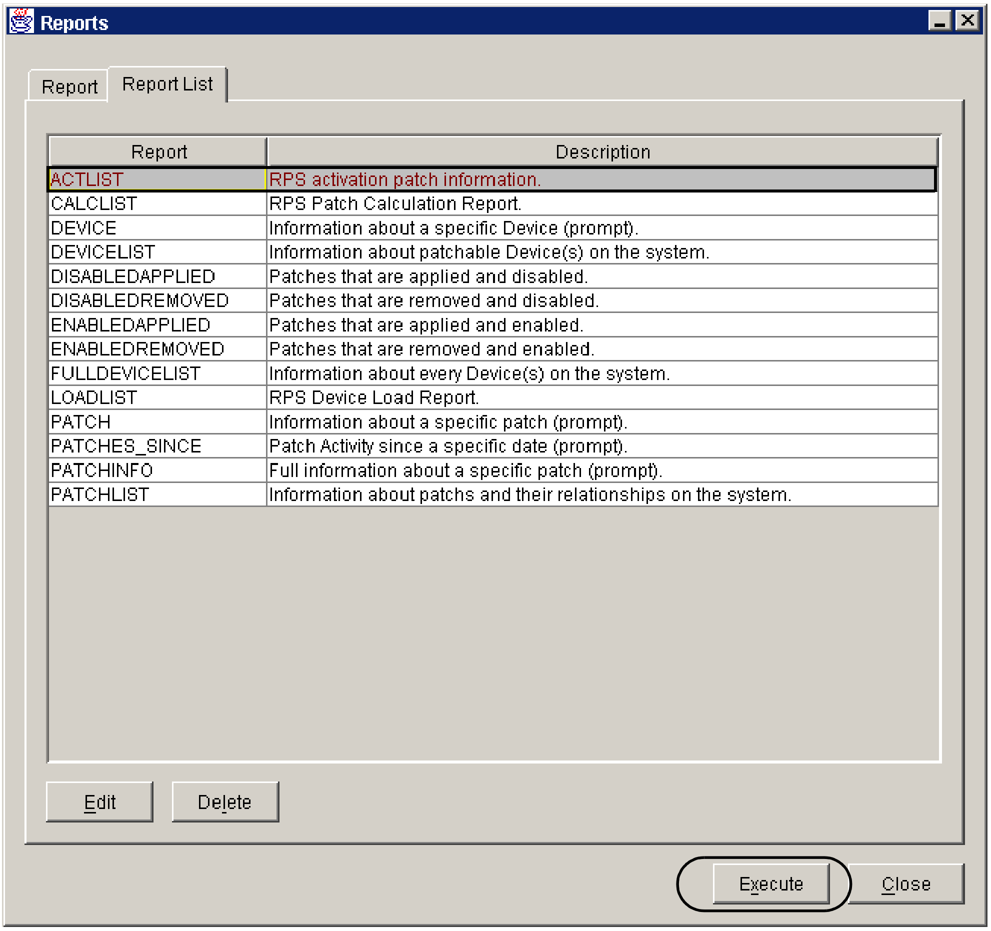


The **Reports** window is displayed.

3 Click the **Report List** tab.



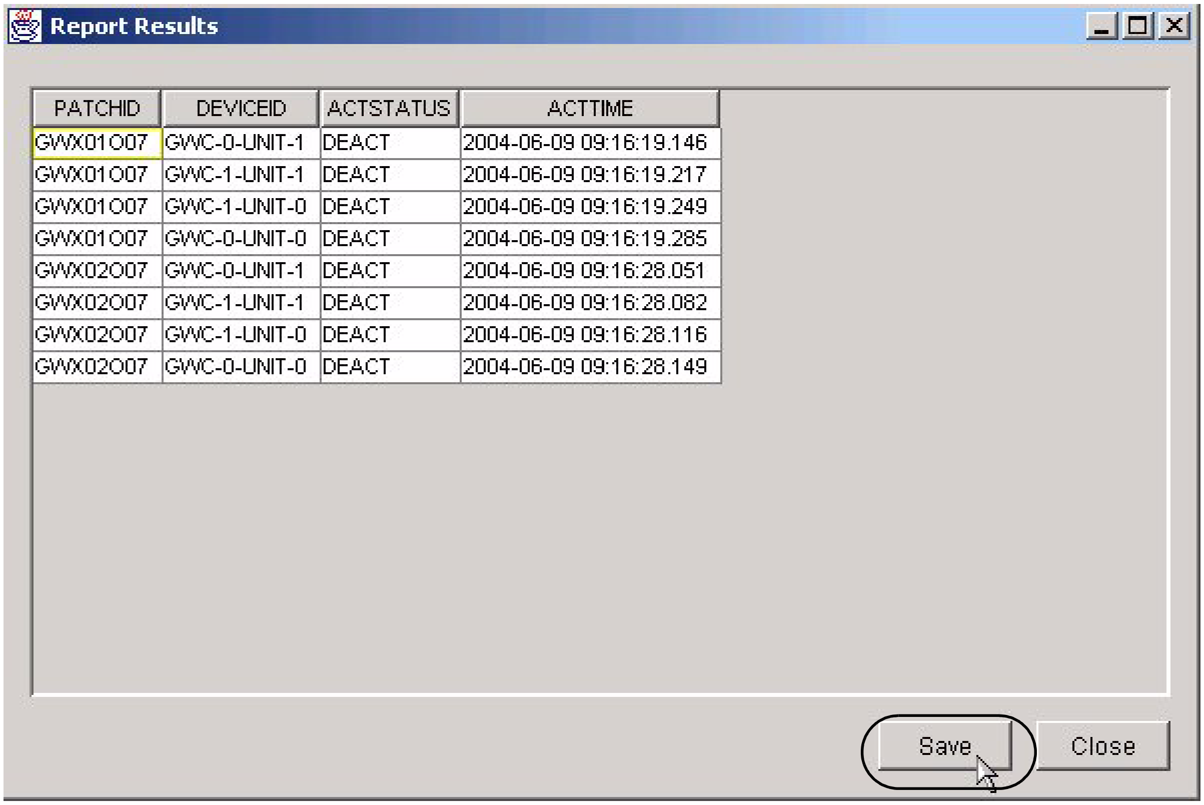
4 Click the **ACTLIST** entry in the **Report** field, then click **Execute**.



Report	Description
ACTLIST	RPS activation patch information.
CALCLIST	RPS Patch Calculation Report.
DEVICE	Information about a specific Device (prompt).
DEVICELIST	Information about patchable Device(s) on the system.
DISABLEDAPPLIED	Patches that are applied and disabled.
DISABLEDREMOVED	Patches that are removed and disabled.
ENABLEDAPPLIED	Patches that are applied and enabled.
ENABLEDREMOVED	Patches that are removed and enabled.
FULLDEVICELIST	Information about every Device(s) on the system.
LOADLIST	RPS Device Load Report.
PATCH	Information about a specific patch (prompt).
PATCHES_SINCE	Patch Activity since a specific date (prompt).
PATCHINFO	Full information about a specific patch (prompt).
PATCHLIST	Information about patchs and their relationships on the system.

5 Review the list of patches displayed, and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and should be activated.

Note: If there are no patches to activate, the system returns a dialog box indicating that the report has “empty results”.

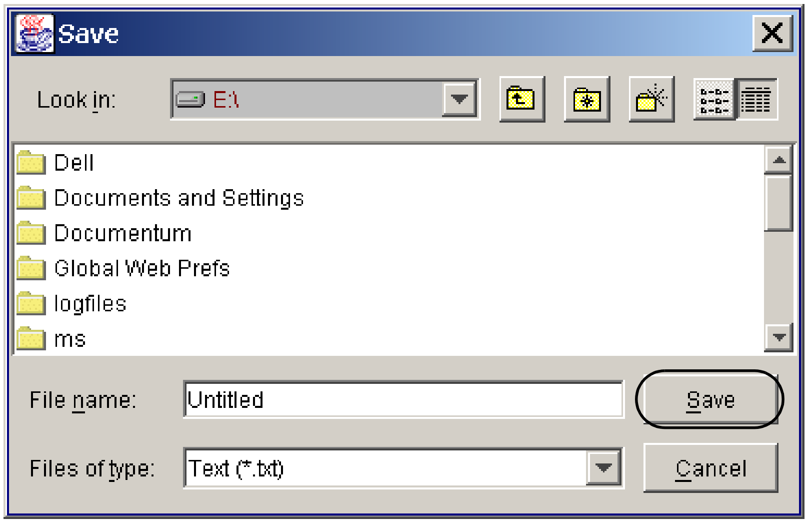


PATCHID	DEVICEID	ACTSTATUS	ACTTIME
GWX01O07	GWC-0-UNIT-1	DEACT	2004-06-09 09:16:19.146
GWX01O07	GWC-1-UNIT-1	DEACT	2004-06-09 09:16:19.217
GWX01O07	GWC-1-UNIT-0	DEACT	2004-06-09 09:16:19.249
GWX01O07	GWC-0-UNIT-0	DEACT	2004-06-09 09:16:19.285
GWX02O07	GWC-0-UNIT-1	DEACT	2004-06-09 09:16:28.051
GWX02O07	GWC-1-UNIT-1	DEACT	2004-06-09 09:16:28.082
GWX02O07	GWC-1-UNIT-0	DEACT	2004-06-09 09:16:28.116
GWX02O07	GWC-0-UNIT-0	DEACT	2004-06-09 09:16:28.149

6 If necessary, save a copy of the report to a text file as follows:

a Click **Save**.

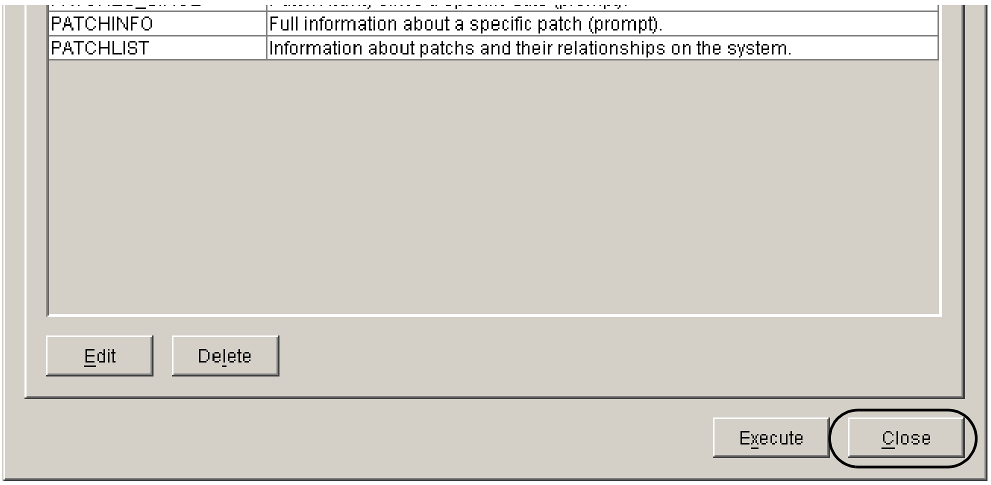
b Type a file name in the **File name:** box, and click **Save**.



File name: Untitled

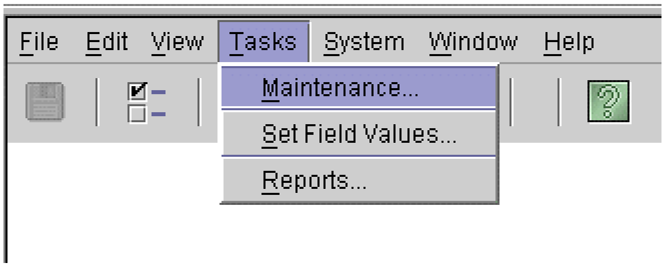
Files of type: Text (*.txt)

7 Click **Close** to close the Reports window.



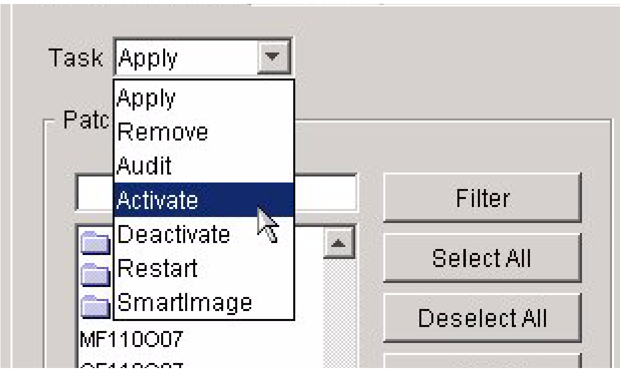
PATCHINFO	Full information about a specific patch (prompt).
PATCHLIST	Information about patchs and their relationships on the system.

8 On the **Tasks** menu, click **Maintenance...**.



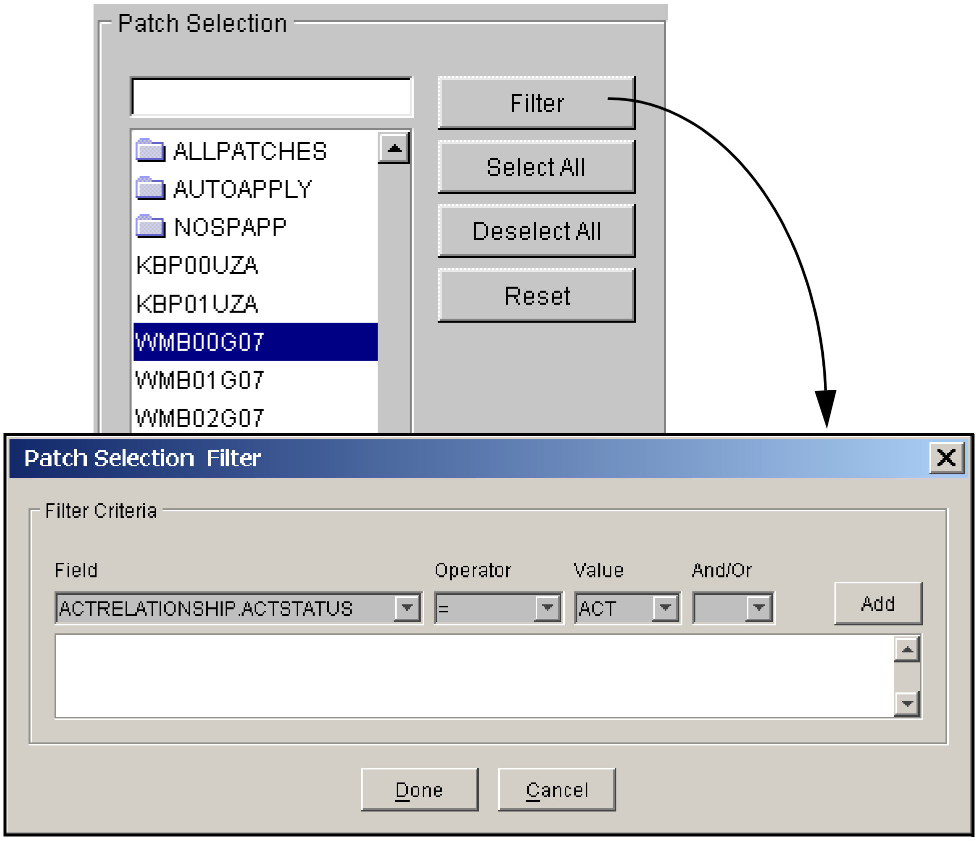
The Maintenance window is displayed.

9 In the **Task** list, click **Activate**.



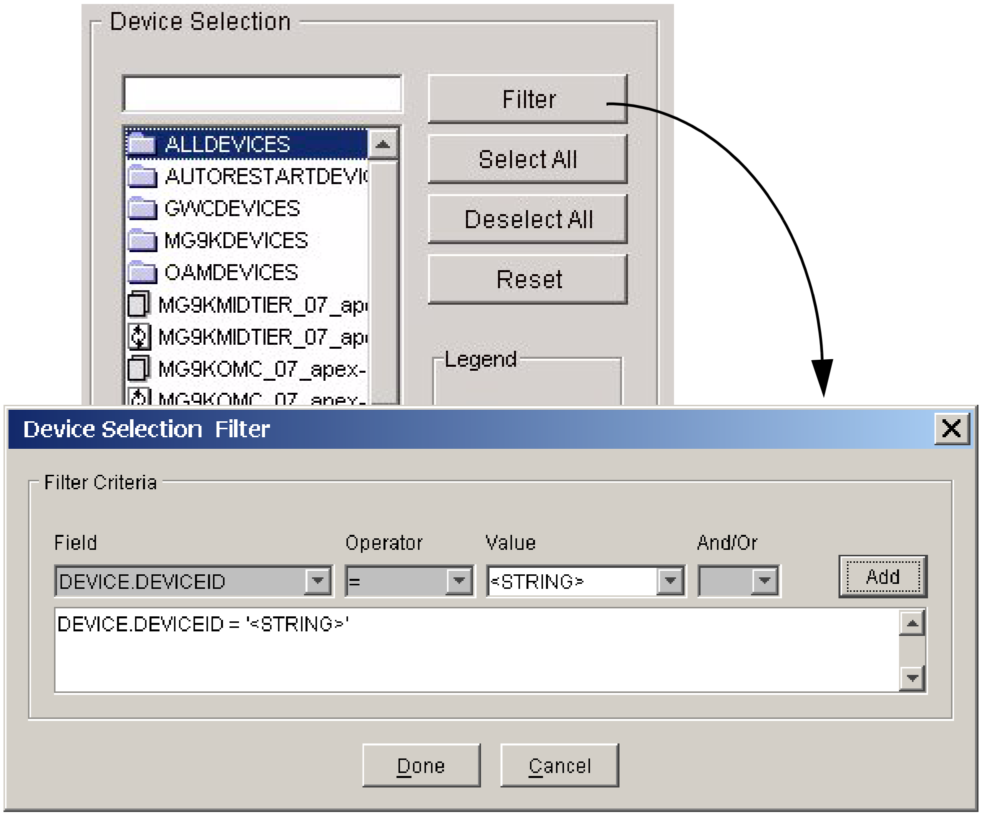
10 In the **Patch Selection** list, select the patch files or patch sets you want to activate, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.

Note: The patches must have a category of ACT.



Field: ACTRELATIONSHIP.ACTSTATUS
Operator: =
Value: ACT
And/Or:

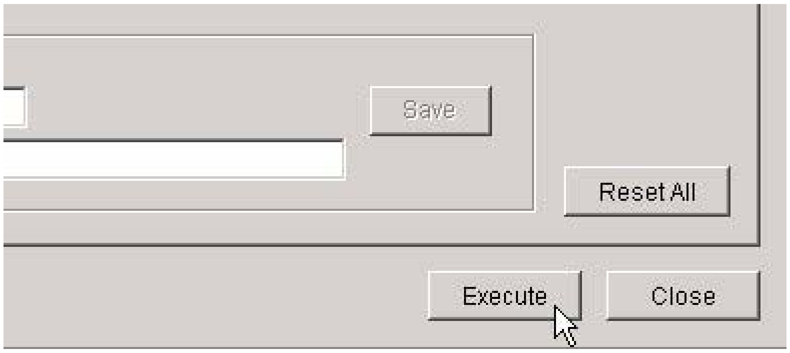
11 In the **Device Selection** list, select the devices or device sets that have the applied patches you want to activate, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.



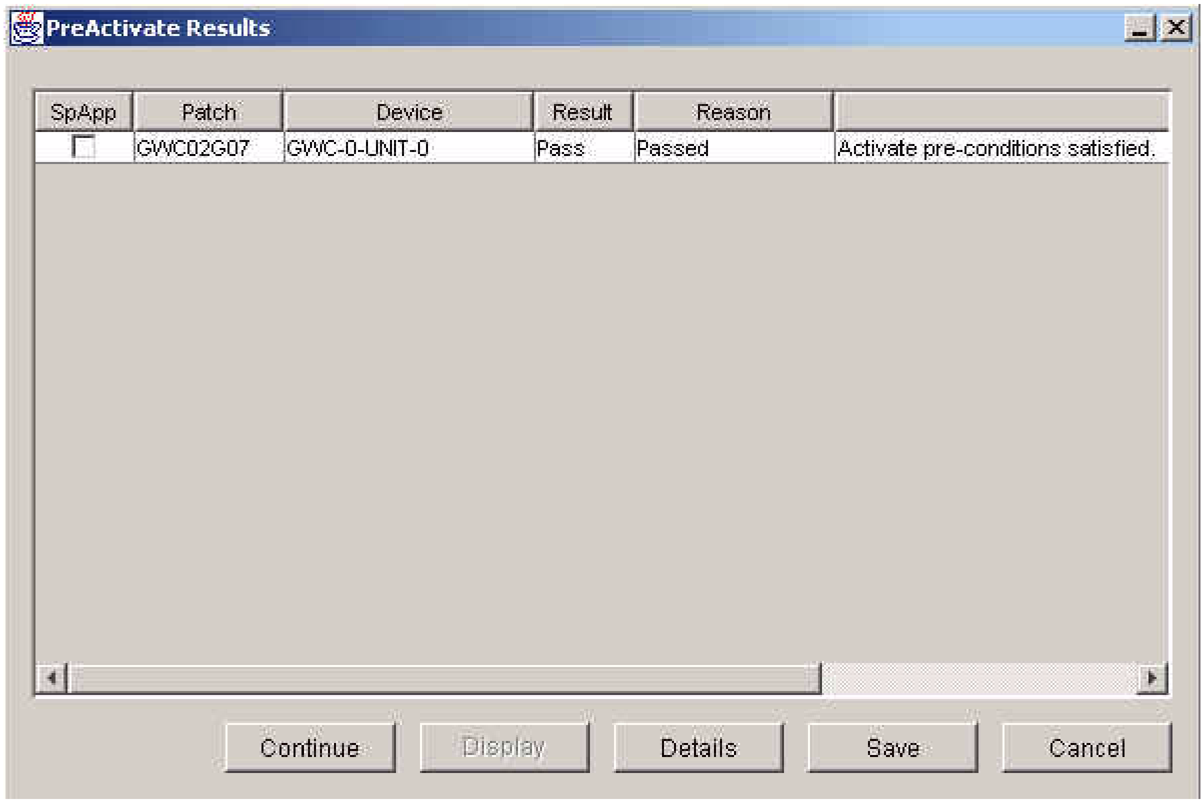
Field: DEVICE.DEVICEID
Operator: =
Value: <STRING>

DEVICE.DEVICEID = '<STRING>'

12 Click **Execute** to begin the patch activation process.



The results of the Pre-activate phase are displayed.



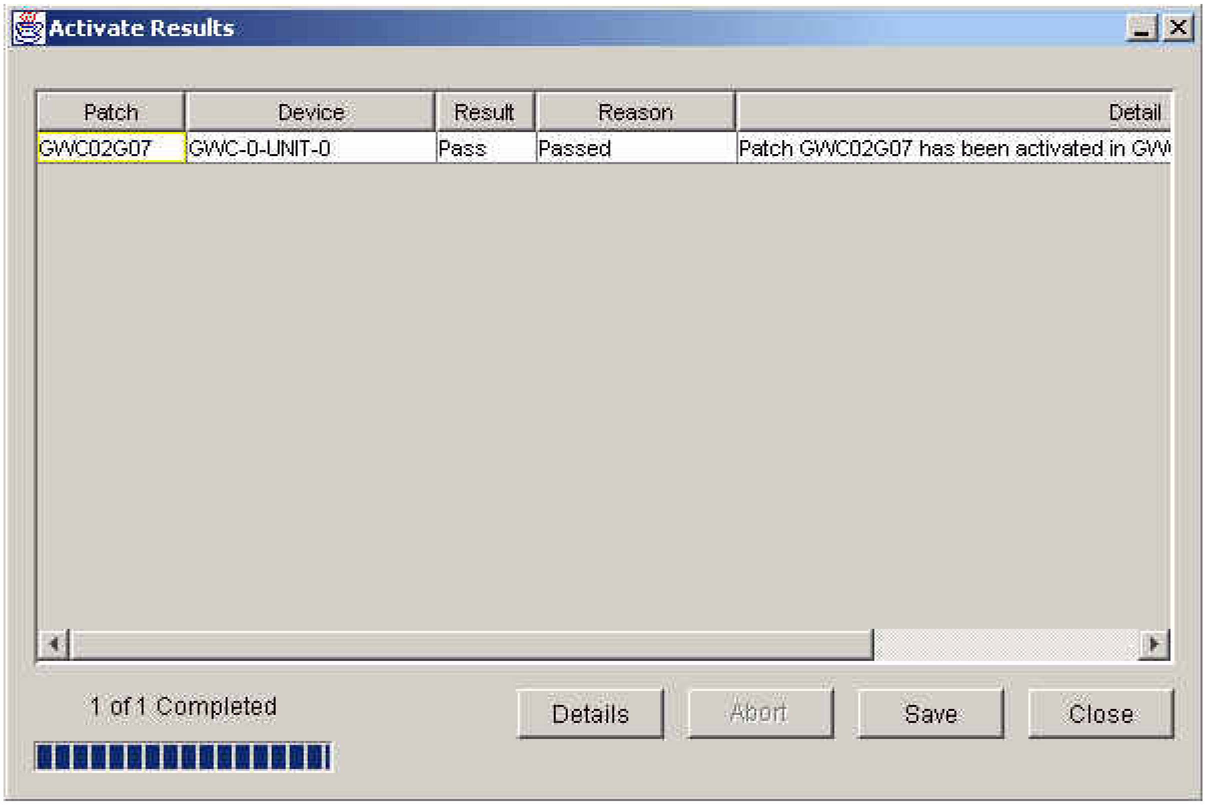
PreActivate Results

SpApp	Patch	Device	Result	Reason	
□	GWC02G07	GWC-0-UNIT-0	Pass	Passed	Activate pre-conditions satisfied.

13 Review the PreActivate Results, then click **Continue** to proceed.

Note: If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Activate Results window is displayed with results added as each action is completed. Failures from the PreActivate phase are also included in the results.



Activate Results

Patch	Device	Result	Reason	Detail
GWC02G07	GWC-0-UNIT-0	Pass	Passed	Patch GWC02G07 has been activated in GW

1 of 1 Completed

14 Click **Save** to save the results to a file, or click **Close**.

Note: If the patches do not successfully activate, abort the patching procedure and contact your next level of support.

15 You have completed this procedure.

Deactivate patches using the NPM

Application

Use this procedure to deactivate one or more ACT category patches using the Network Patch Manager (NPM). You can deactivate patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 122
- Using the NPM GUI on page 123

Note: Currently, only GWC can have ACT category patches.

Prerequisites

You can deactivate a patch if the following criteria apply:

- the patch to be deactivated has been identified by your support team and Nortel as being applicable for your site and be recommended for deactivation
- the patch has been activated
- the patch is not on hold

CAUTION

Do not deactivate patches for your components that have not been identified as needing deactivation without first consulting with your network administrator and your Nortel customer support representative. Failure to do so can result in partial loss of service.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 in this document, if required.

At the NPM CLUI

2 Query the NPM for a list of patches that are activated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime. If no patches are in the actlist, then the NPM responds with the message “Empty Results”.

3 Deactivate one or more patches for one or more devices by typing

```
npm> deactivate <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to deactivate - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices

is a list of one or more device IDs for which you want to deactivate the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and deactivates them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example

`npm> deactivate` ACT02GAX in GWC-8-UNIT-1

4 When prompted, press the Enter key.

5 Query the NPM to verify the patches are deactivated by typing

```
npm> q actlist
```

The NPM responds by displaying a list of patches and their status in the following order: patchid, deviceid, actstatus, acttime.

6 Verify from the list that the desired patches are deactivated.

> ***Note:*** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

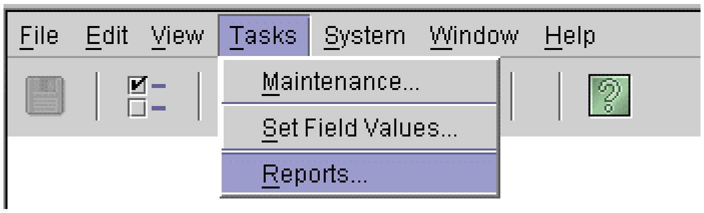
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 in this document, if required.

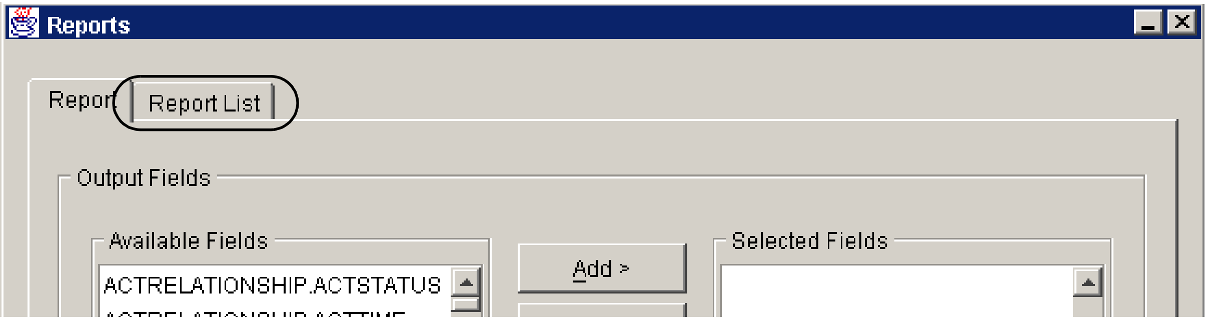
At the NPM GUI

2 On the **Tasks** menu, click **Reports...**.

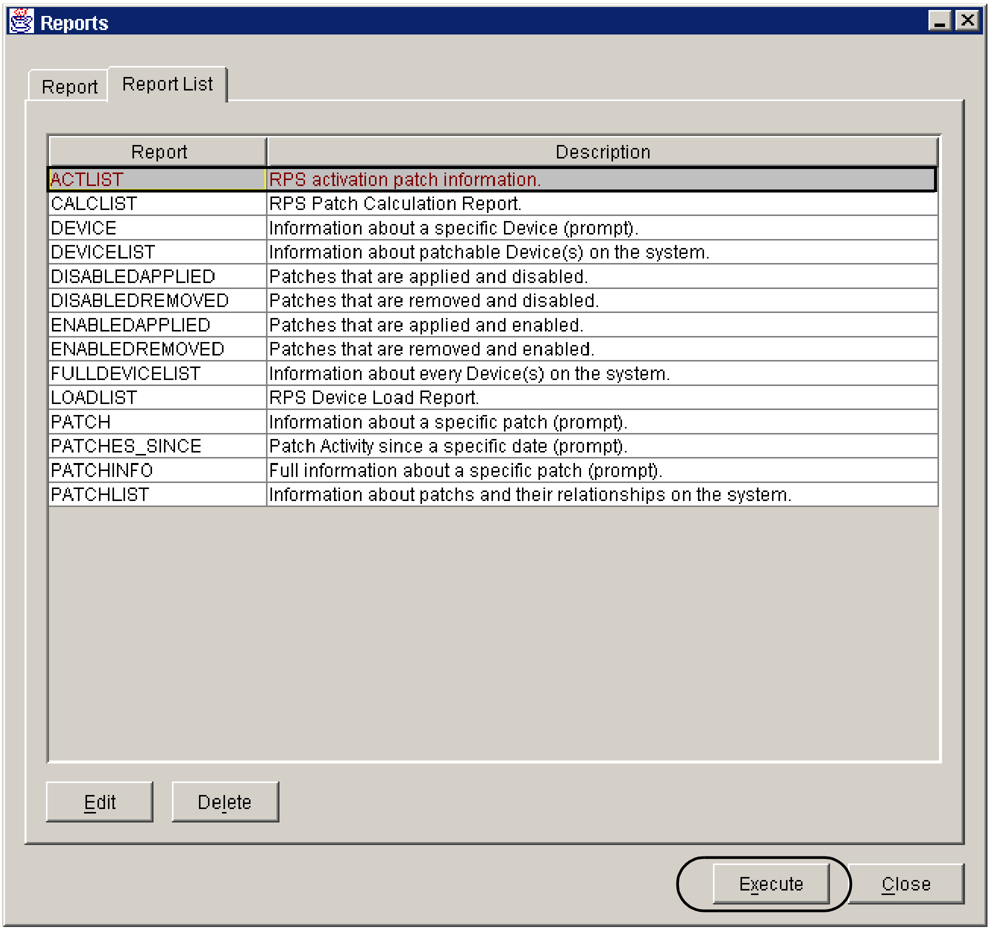


The Reports window is displayed.

3 Click the **Report List** tab.



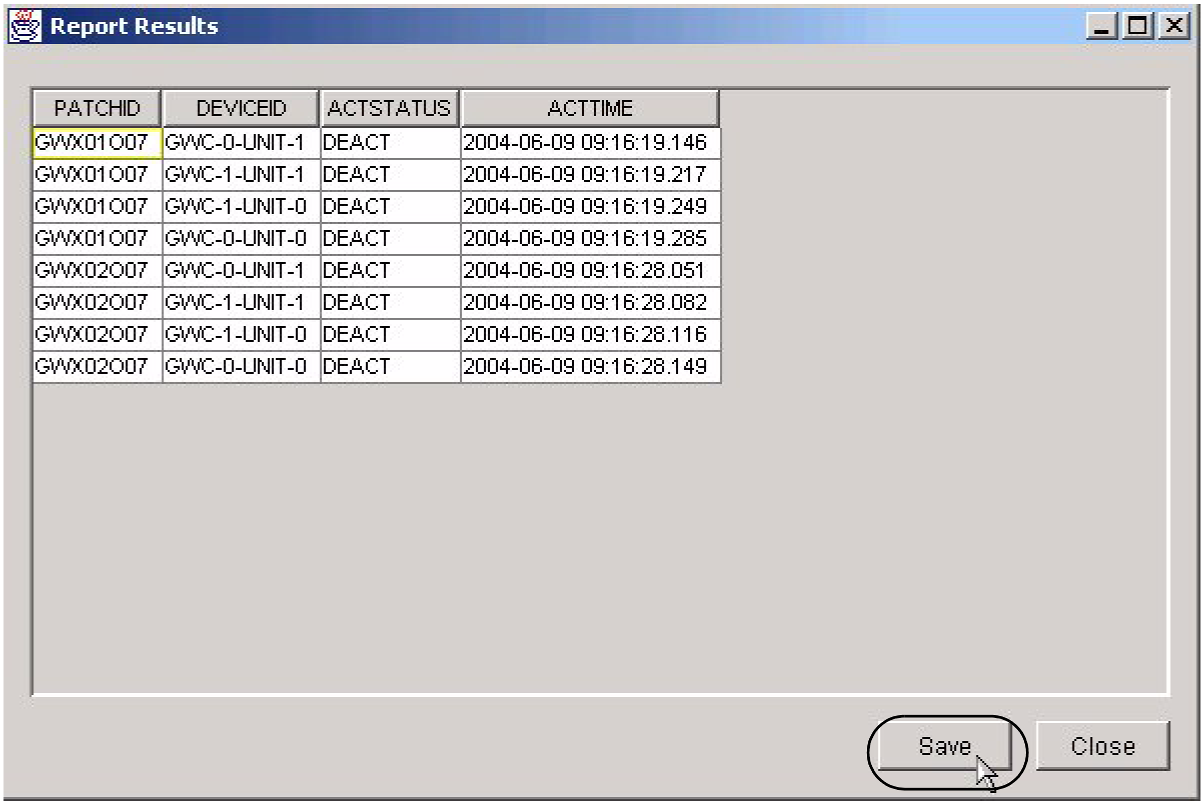
4 Click the **ACTLIST** entry in the **Report** field, then click **Execute**.



Report	Description
ACTLIST	RPS activation patch information.
CALCLIST	RPS Patch Calculation Report.
DEVICE	Information about a specific Device (prompt).
DEVICELIST	Information about patchable Device(s) on the system.
DISABLEDAPPLIED	Patches that are applied and disabled.
DISABLEDREMOVED	Patches that are removed and disabled.
ENABLEDAPPLIED	Patches that are applied and enabled.
ENABLEDREMOVED	Patches that are removed and enabled.
FULLDEVICELIST	Information about every Device(s) on the system.
LOADLIST	RPS Device Load Report.
PATCH	Information about a specific patch (prompt).
PATCHES_SINCE	Patch Activity since a specific date (prompt).
PATCHINFO	Full information about a specific patch (prompt).
PATCHLIST	Information about patchs and their relationships on the system.

5 Review the list of patches displayed and note which are activated and which are deactivated. Consult with your Nortel customer support representative to determine which patch files are applicable to your site configuration and should be deactivated.

Note: If there are no patches to deactivate, the system returns a dialog box indicating that the report has “empty results”.

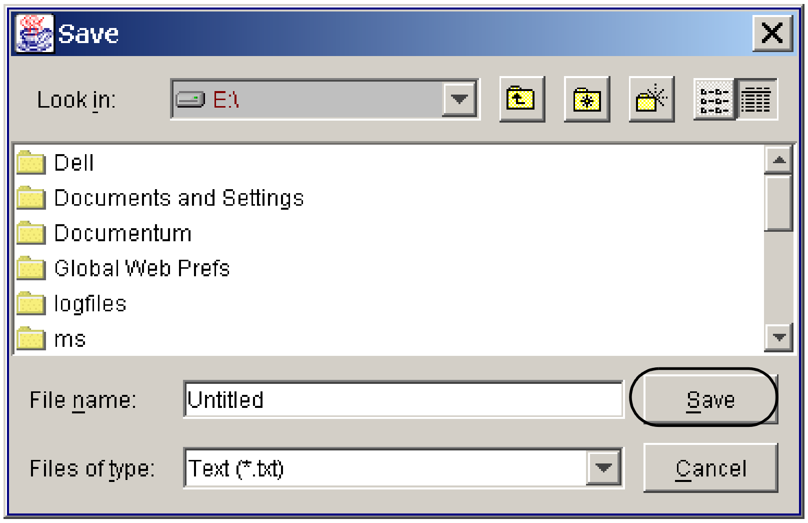


PATCHID	DEVICEID	ACTSTATUS	ACTTIME
GWX01007	GWC-0-UNIT-1	DEACT	2004-06-09 09:16:19.146
GWX01007	GWC-1-UNIT-1	DEACT	2004-06-09 09:16:19.217
GWX01007	GWC-1-UNIT-0	DEACT	2004-06-09 09:16:19.249
GWX01007	GWC-0-UNIT-0	DEACT	2004-06-09 09:16:19.285
GWX02007	GWC-0-UNIT-1	DEACT	2004-06-09 09:16:28.051
GWX02007	GWC-1-UNIT-1	DEACT	2004-06-09 09:16:28.082
GWX02007	GWC-1-UNIT-0	DEACT	2004-06-09 09:16:28.116
GWX02007	GWC-0-UNIT-0	DEACT	2004-06-09 09:16:28.149

6 If necessary, save a copy of the report to a text file as follows:

a Click **Save**.

b Type a file name in the **File name:** box, and click **Save**.



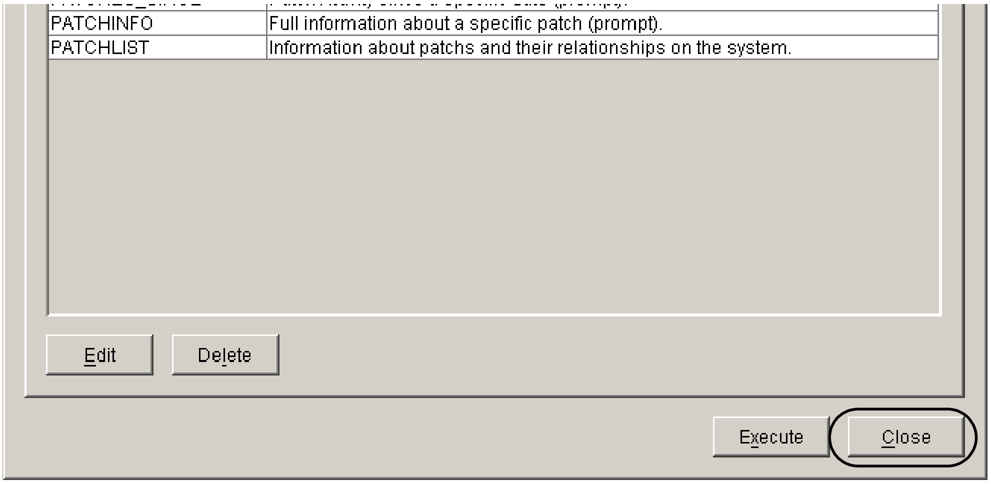
Look in: E:\

Dell
Documents and Settings
Documentum
Global Web Prefs
logfiles
ms

File name: Untitled

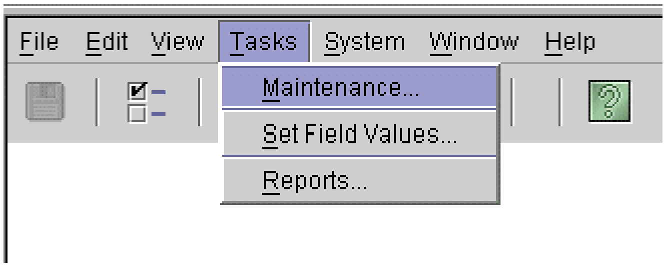
Files of type: Text (*.txt)

7 Click **Close** to close the Reports window.



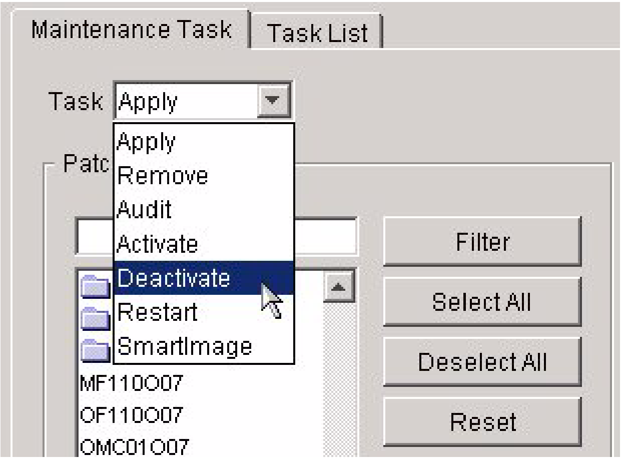
PATCHINFO	Full information about a specific patch (prompt).
PATCHLIST	Information about patchs and their relationships on the system.

8 On the **Tasks** menu, click **Maintenance...**.



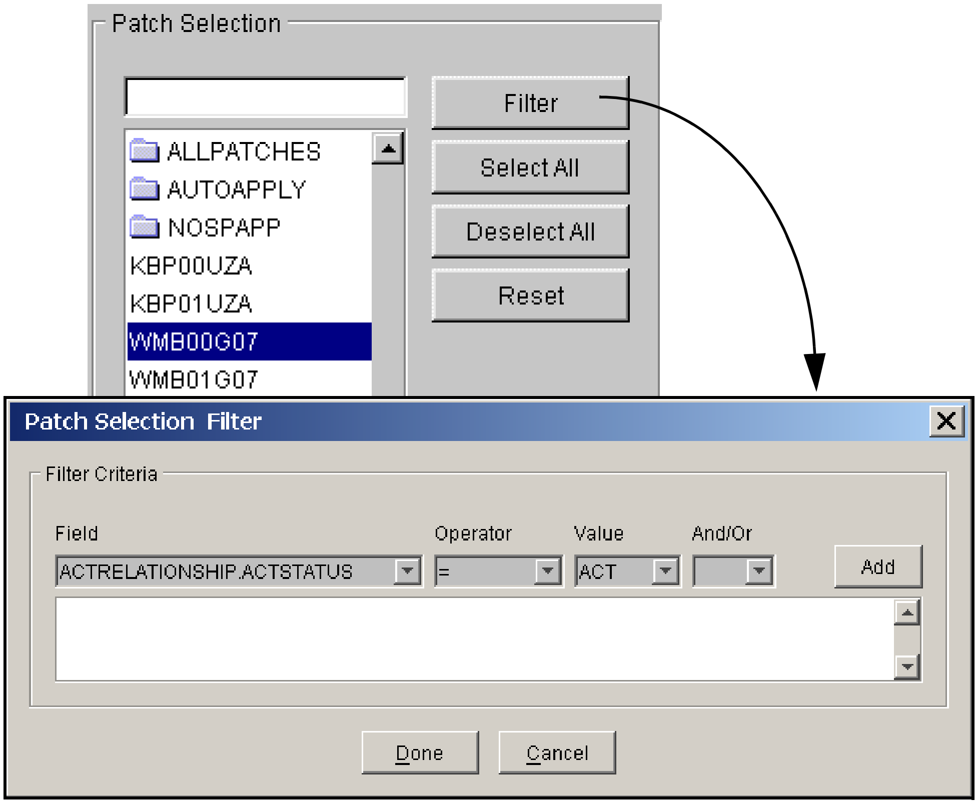
The Maintenance window is displayed.

9 In the **Task** list, click **Deactivate**.



Task Apply

10 In the **Patch Selection** list, select the patch files or patch sets you want to deactivate, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



Patch Selection

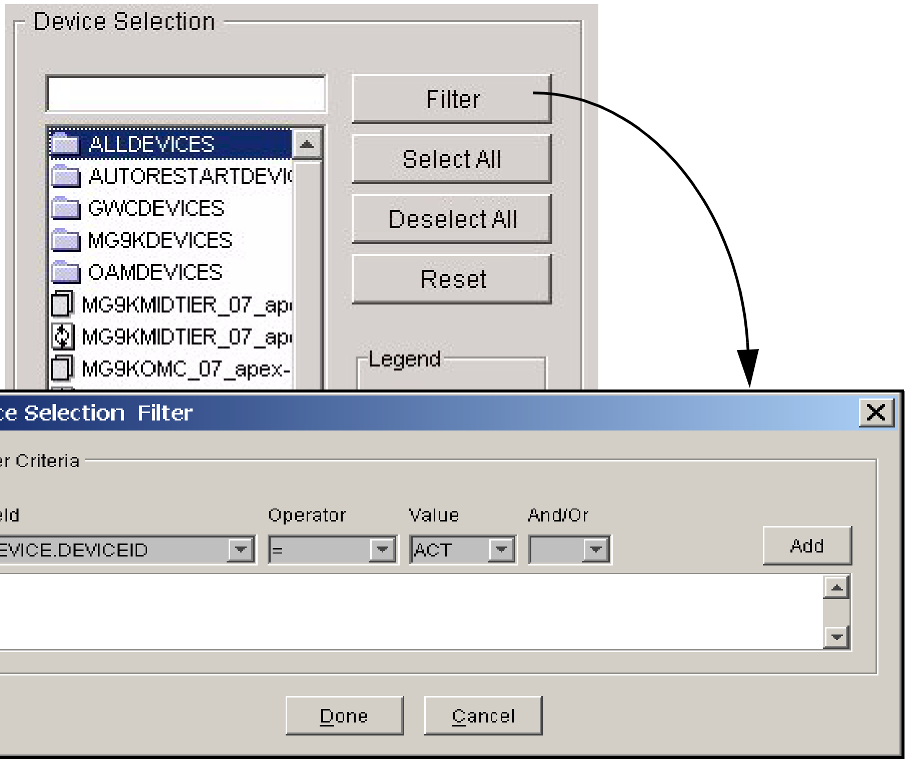
- ALLPATCHES
- AUTOAPPLY
- NOSPAPP
- KBP00UZA
- KBP01UZA
- WMB00G07
- WMB01G07

Patch Selection Filter

Filter Criteria

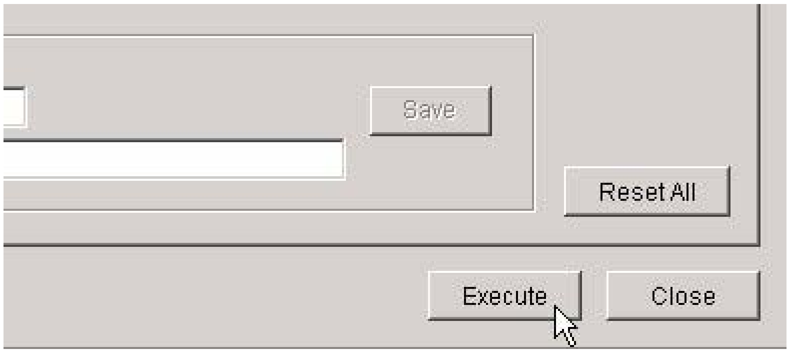
Field	Operator	Value	And/Or
ACTRELATIONSHIP.ACTSTATUS	=	ACT	

11 In the **Device Selection** list, select the devices or device sets for which you are deactivating the patches, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.

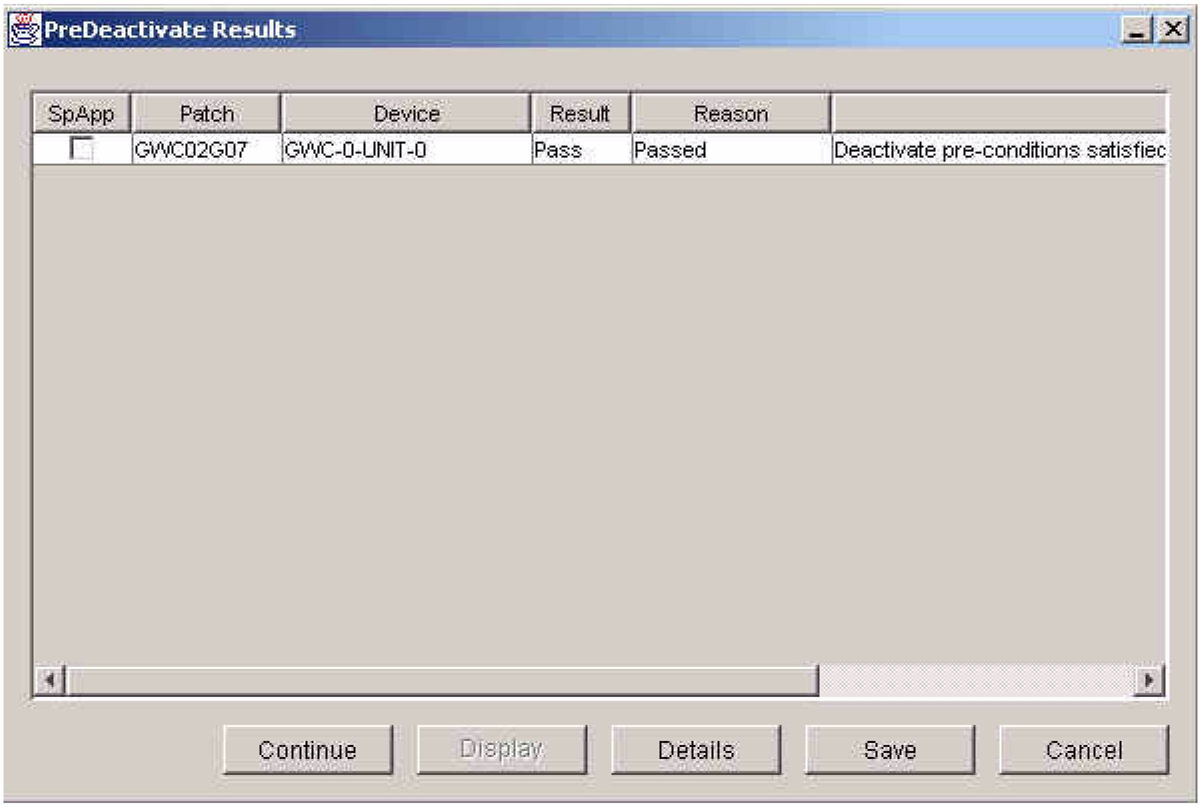


Field: DEVICE.DEVICEID Operator: = Value: ACT

12 Click **Execute** to begin the patch deactivation process.



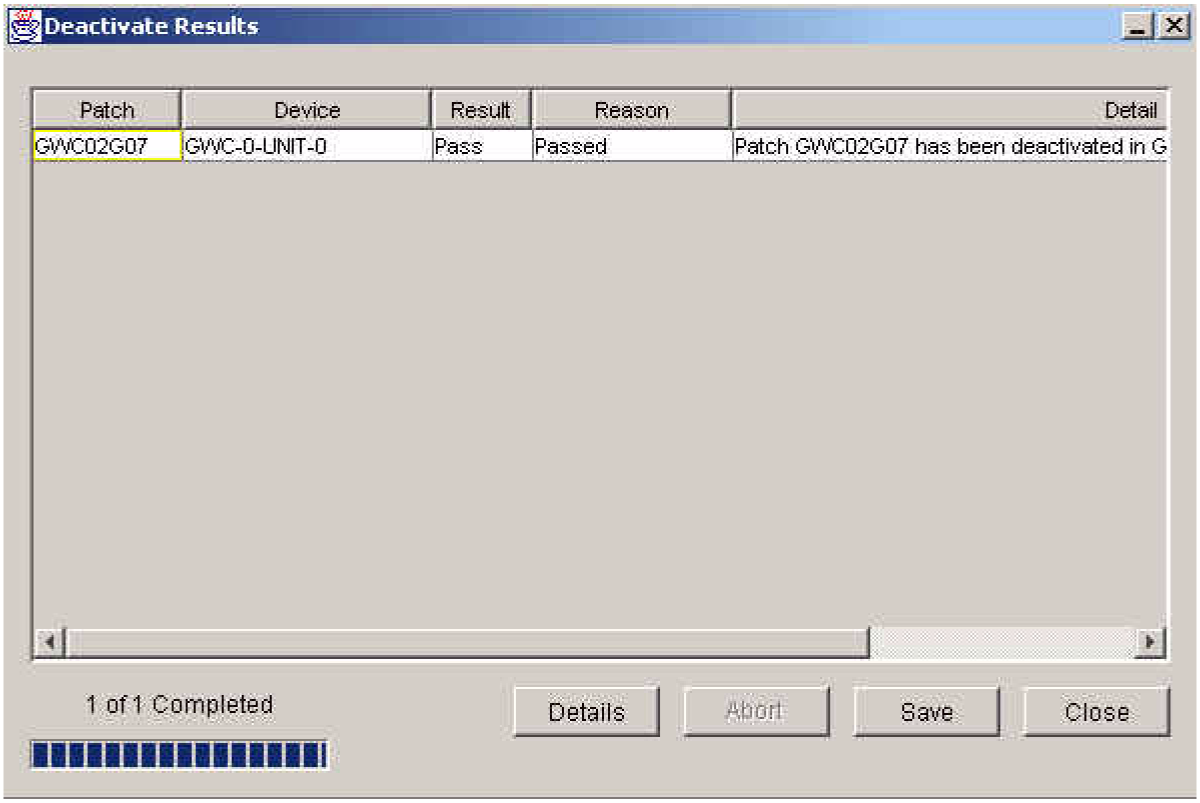
The results of the Pre-deactivate phase are displayed.



SpApp	Patch	Device	Result	Reason	
□	GWC02G07	GWC-0-UNIT-0	Pass	Passed	Deactivate pre-conditions satisfiec

13 Review the PreDeactivate Results, then click **Continue** to proceed.

The Deactivate Results window is displayed with results added as each action is completed. Failures from the PreDeactivate phase are also included in the results.



Patch	Device	Result	Reason	Detail
GWC02G07	GWC-0-UNIT-0	Pass	Passed	Patch GWC02G07 has been deactivated in G

14 Click **Save** to save the results to a file, or click **Close**.

> ***Note:*** If the patches do not successfully deactivate, abort the patching procedure and contact your next level of support.

15 You have completed this procedure.

Remove patches using the NPM

Application

Use this procedure to remove patches using the Network Patch Manager (NPM). You can remove patches using one of the following two NPM interfaces:

- Using the NPM CLUI on page 132
- Using the NPM GUI on page 135

Prerequisites

Before you remove ACT category patches, you must first deactivate the patches. Refer to procedure Deactivate patches using the NPM on page 121 if required.

Ensure the patch is not on hold.

You must be assigned to user group “emsadm” to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on a Sun server” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

Action

Perform the steps under Using the NPM CLUI or Using the NPM GUI to complete this procedure.

Using the NPM CLUI

At your workstation

1 Access the NPM CLUI. Refer to procedure Access the Network Patch Manager CLUI on page 82 if required.

At the NPM CLUI

2 Remove one or more patches from one or more devices by typing

```
npm> remove <patches> [in <devices>]
```

and pressing the Enter key.

where

patches
is a list of one or more patch IDs you want to remove - the syntax is

<patchid> [<patchid>...<patchid>]

or

SET <predefined set definition>

devices
is a list of one or more device IDs from which you want to remove the patches (if you do not specify one or more device IDs, the NPM determines to which devices the patches are applicable, and removes them) - the syntax is

<deviceid> [<deviceid>...<deviceid>]

or

SET <predefined set definition>

Example

```
npm> remove ACT02GAX in GWC-8-UNIT-1
```

3 When prompted, press the Enter key.

4 Generate a device query report to verify the patches are removed by typing

```
npm> q device
```

5 Enter the device name in the format **<deviceid>** that you input in step 2.

A device report of known patch activity for the particular device associated with the <device id> is returned.

6 Verify from the report that the desired patches are removed.

Note: If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

7 You have completed this procedure.

If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure “Restarting a device using the NPM” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

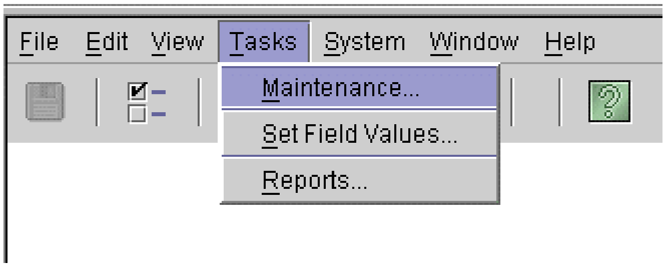
Using the NPM GUI

At your workstation

1 Access the NPM GUI. Refer to procedure Launch CS 2000 Management Tools client applications on page 69 if required.

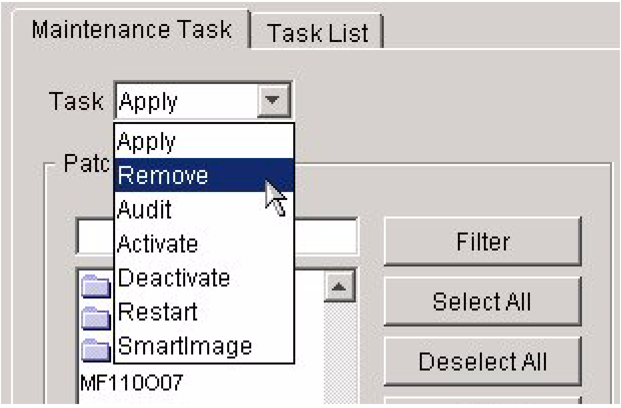
At the NPM GUI

2 On the **Tasks** menu, click **Maintenance...**.

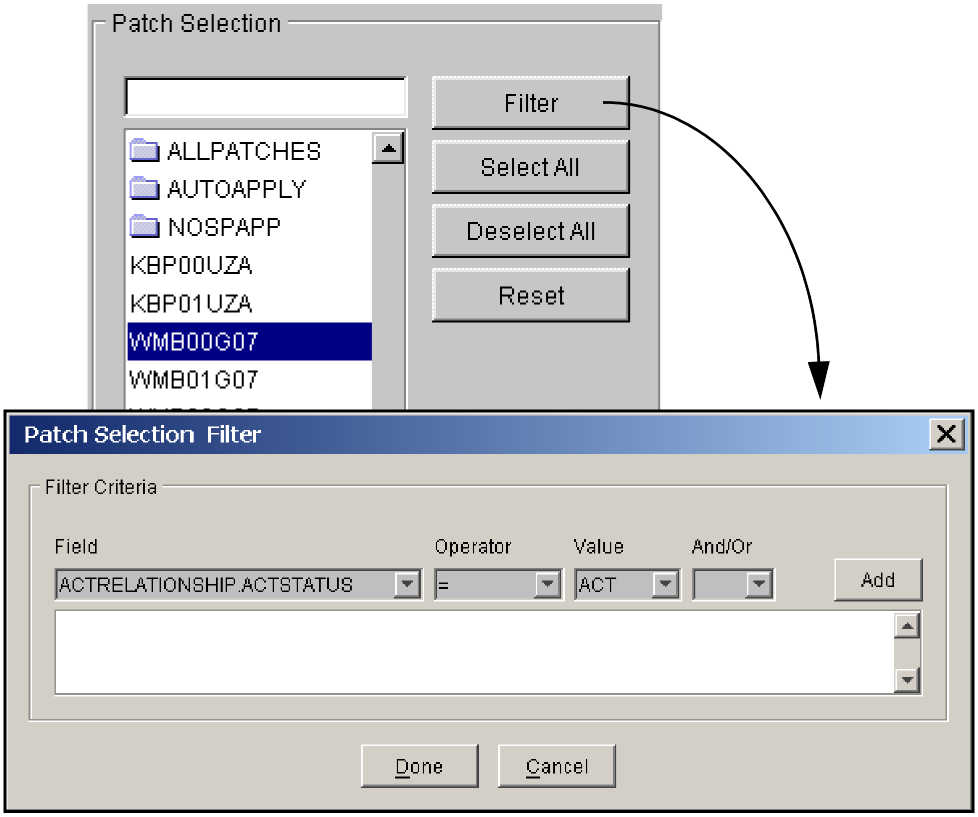


The Maintenance window is displayed.

3 In the **Task** list, click **Remove**.



4 In the **Patch Selection** list, select the patch files or patch sets you want to remove from the Patch Selection list, or click **Filter** to configure a filtering criteria in the **Patch Selection Filter** dialog box.



Patch Selection

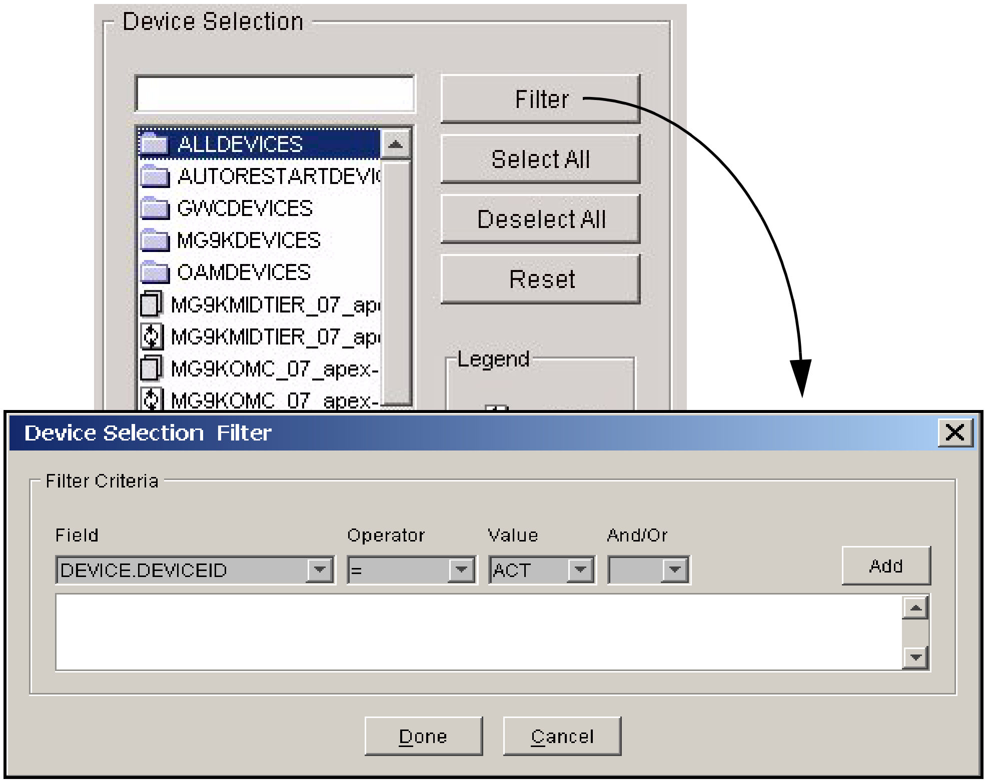
ALLPATCHES
AUTOAPPLY
NOSPAPP
KBP00UZA
KBP01UZA
WMB00G07
WMB01G07

Patch Selection Filter

Filter Criteria

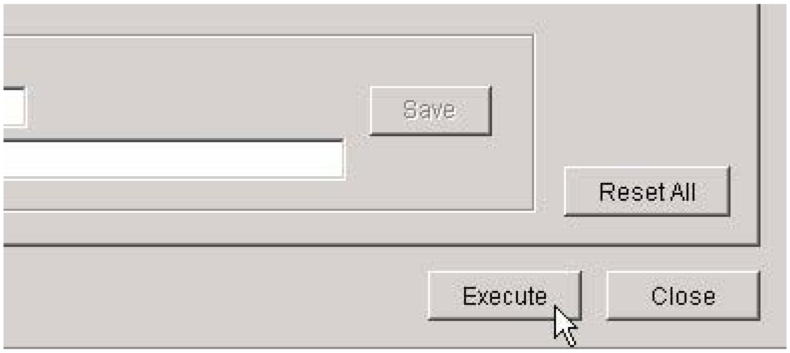
Field: ACTRELATIONSHIP.ACTSTATUS
Operator: =
Value: ACT
And/Or:

5 In the **Device Selection** list, select the devices or device sets from which the patches will be removed, or click **Filter** to configure a filtering criteria in the **Device Selection Filter** dialog box.

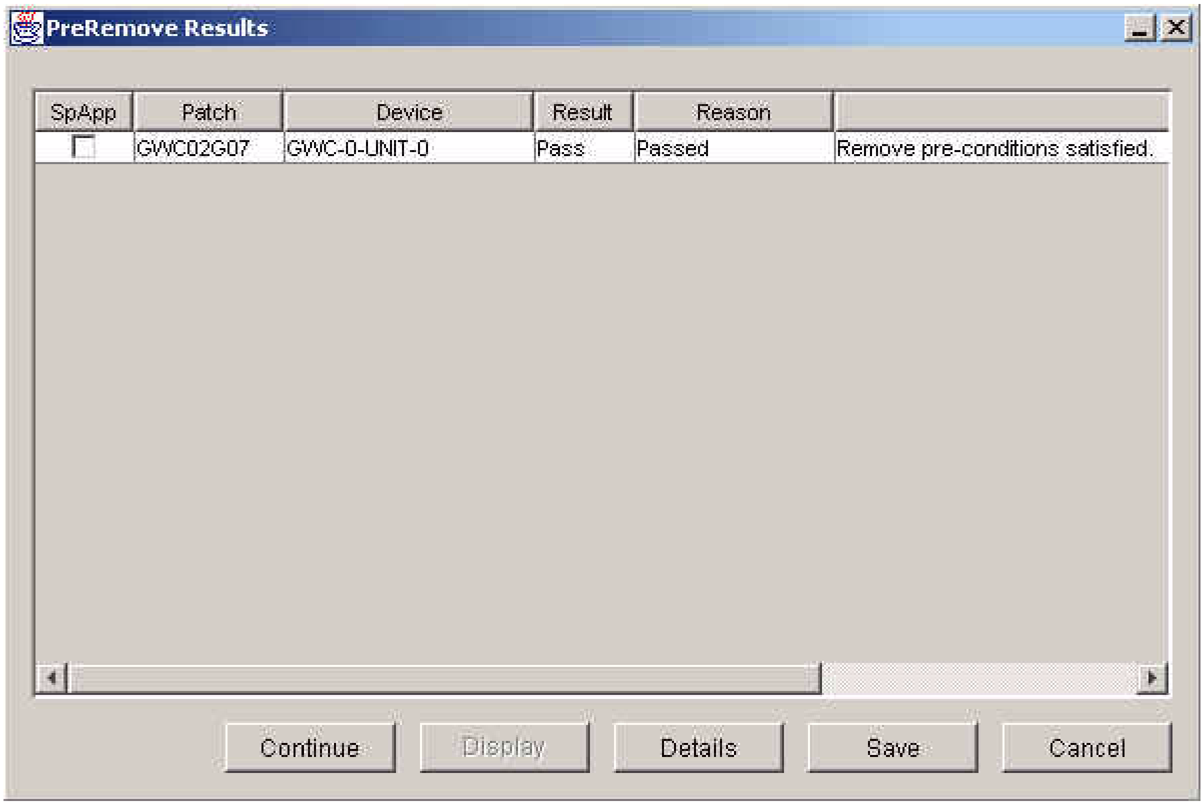


Field: DEVICE.DEVICEID
Operator: =
Value: ACT
And/Or:

6 Click **Execute** to begin the patch removal process.



The results of the PreRemove phase are displayed.

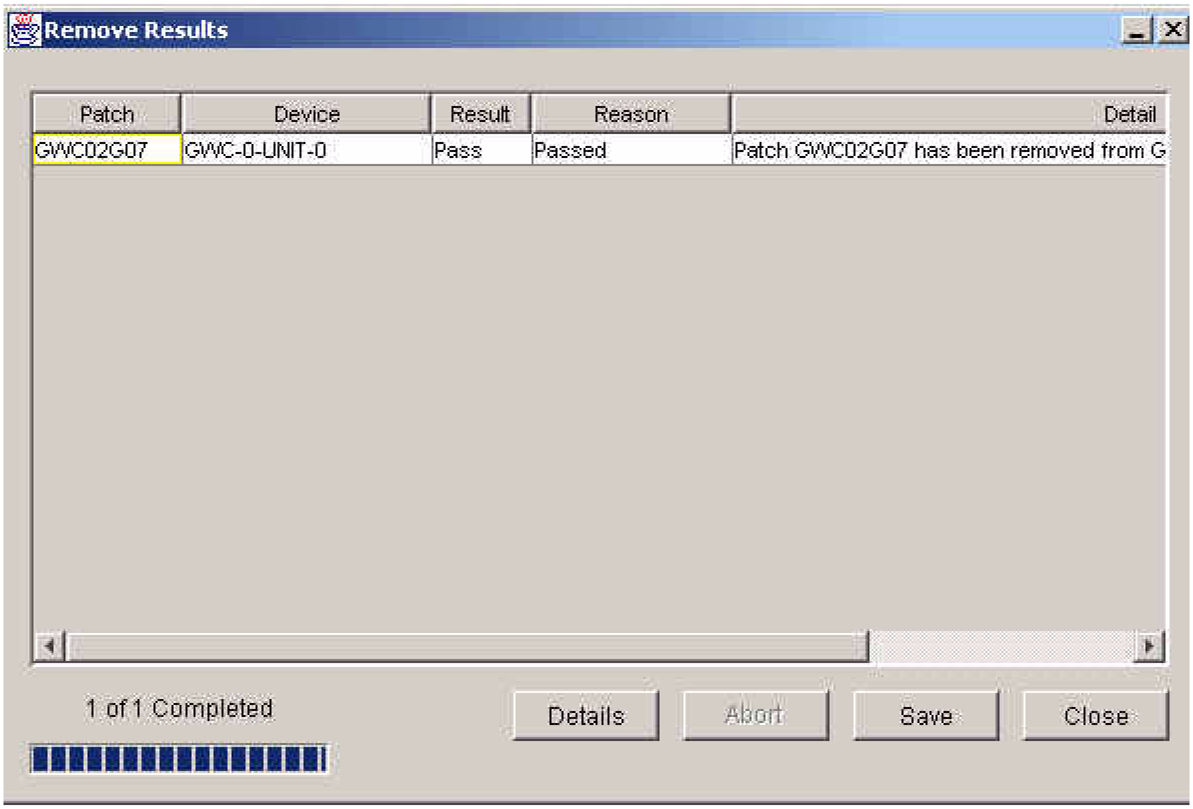


SpApp	Patch	Device	Result	Reason	
□	GWC02G07	GWC-0-UNIT-0	Pass	Passed	Remove pre-conditions satisfied.

7 Review the PreRemove Results, then **Continue** to proceed.

> ***Note:*** If the SpApp field is checked for any patch, the Special Application instructions for each patch must be displayed before the system will allow the request to continue. If the patch is listed in multiple operations, the SpApp need only be viewed once.

The Remove Results window is displayed with results added as each action is completed. Failures from the PreRemove phase are also included in the results.



Remove Results

Patch	Device	Result	Reason	Detail
GWC02G07	GWC-0-UNIT-0	Pass	Passed	Patch GWC02G07 has been removed from G

1 of 1 Completed

8 Click **Save** to save the results to a file, or click **Close**.

> ***Note:*** If the patches do not successfully remove, abort the patching procedure and contact your next level of support.

9 You have completed this procedure.

If you removed patches from any of the following devices, you need to restart the device in order to disable the patches on the device:

- Integrated Element Management System (EMS)
- Integrated EMS security component
- Patching Server Element (PSE)
- CS 2000 SAM21 Manager
- Succession Element Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Media Gateway (MG) 9000 Manager
- Network Patch Manager (NPM)

To restart a device, refer to procedure “Restarting a device using the NPM” in the Solutions Upgrades NTP NN10261-450 (ATM) or NN10344-450 (IP).

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 159 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.

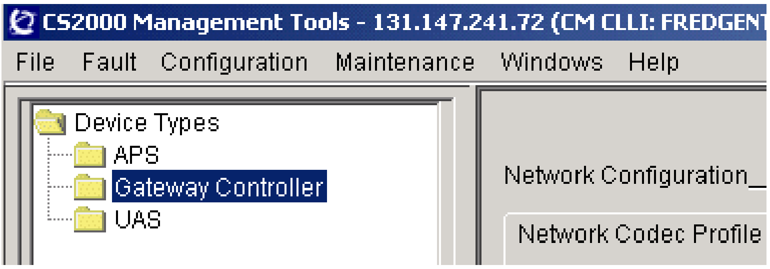
Example

```
# cp pgc06as.imag pgc06as.imag.bak
```

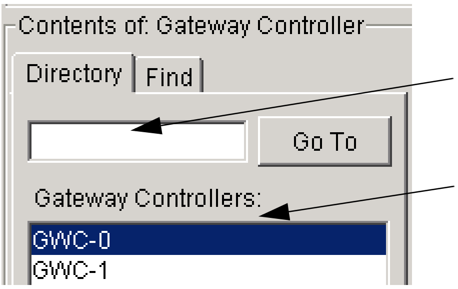
Note: You can use any name for the backup file name.

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.



Type a GWC node number here,

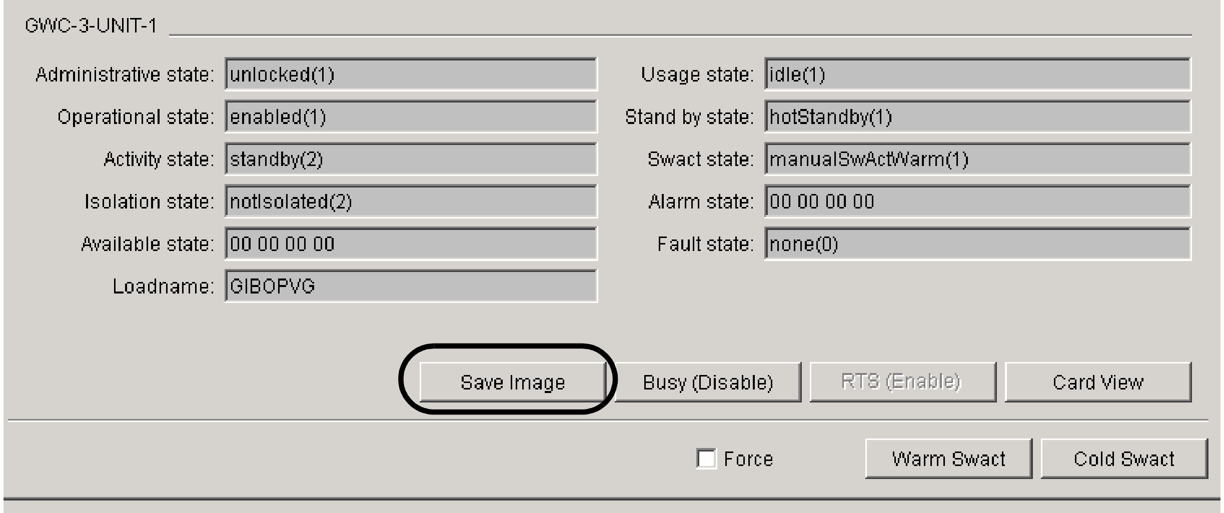
or

Select a GWC node from the list of provisioned GWC nodes.

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.


GWC-3-UNIT-1

Administrative state: unlocked(1)

Operational state: enabled(1)

Activity state: standby(2)

Isolation state: notIsolated(2)

Available state: 00 00 00 00

Loadname: GIBOPVG

Usage state: idle(1)

Stand by state: hotStandby(1)

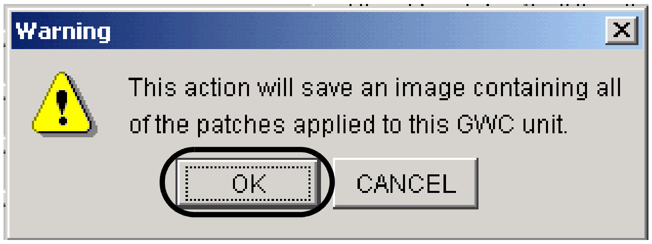
Swact state: manualSwActWarm(1)

Alarm state: 00 00 00 00

Fault state: none(0)

□ Force

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**.


Warning

This action will save an image containing all of the patches applied to this GWC unit.

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

CAUTION

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

8 This procedure is complete.

Note 1: To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade procedure on page 4.

Note 2: To return to the Overall GWC downgrade procedure, refer to Overall GWC downgrade procedure on page 7.

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 (SDM) or Core and Billing Manager (CBM) is different from the firmware version on one or more GWC cards.

When to use this procedure

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

> ***Note:*** This procedure flashes the firmware on the GWC card only if the version of the firmware on the CS 2000 Core Manager or CBM is different from the firmware version on the card. If you need to flash the firmware on a card that contains the same version of the firmware as the CS 2000 Core Manager or CBM, then refer to Force a firmware flash of a GWC card on page 151 in this NTP.

Prerequisites

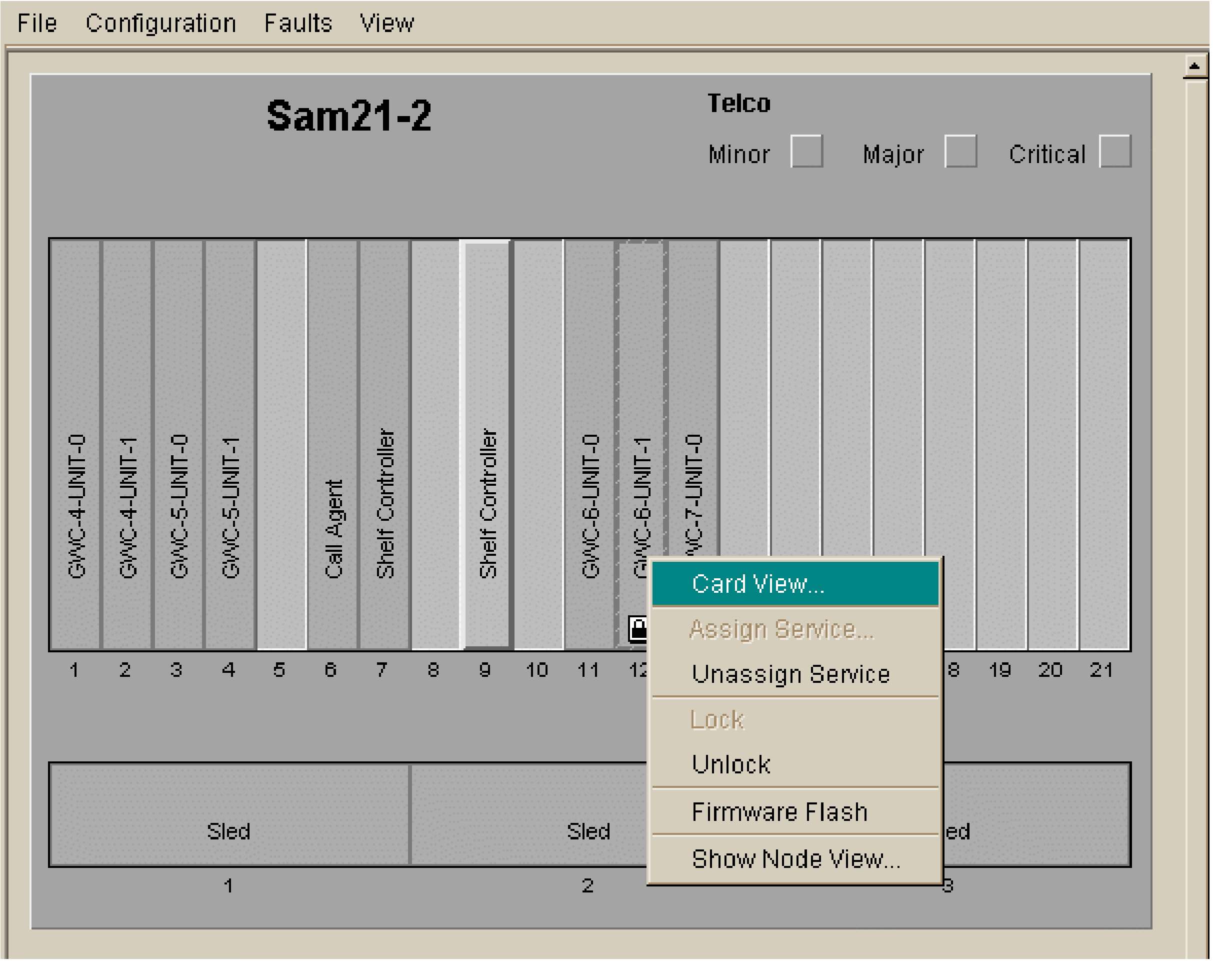
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in the Gateway Controller Security and Administration NTP, NN10213-611.

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

Action

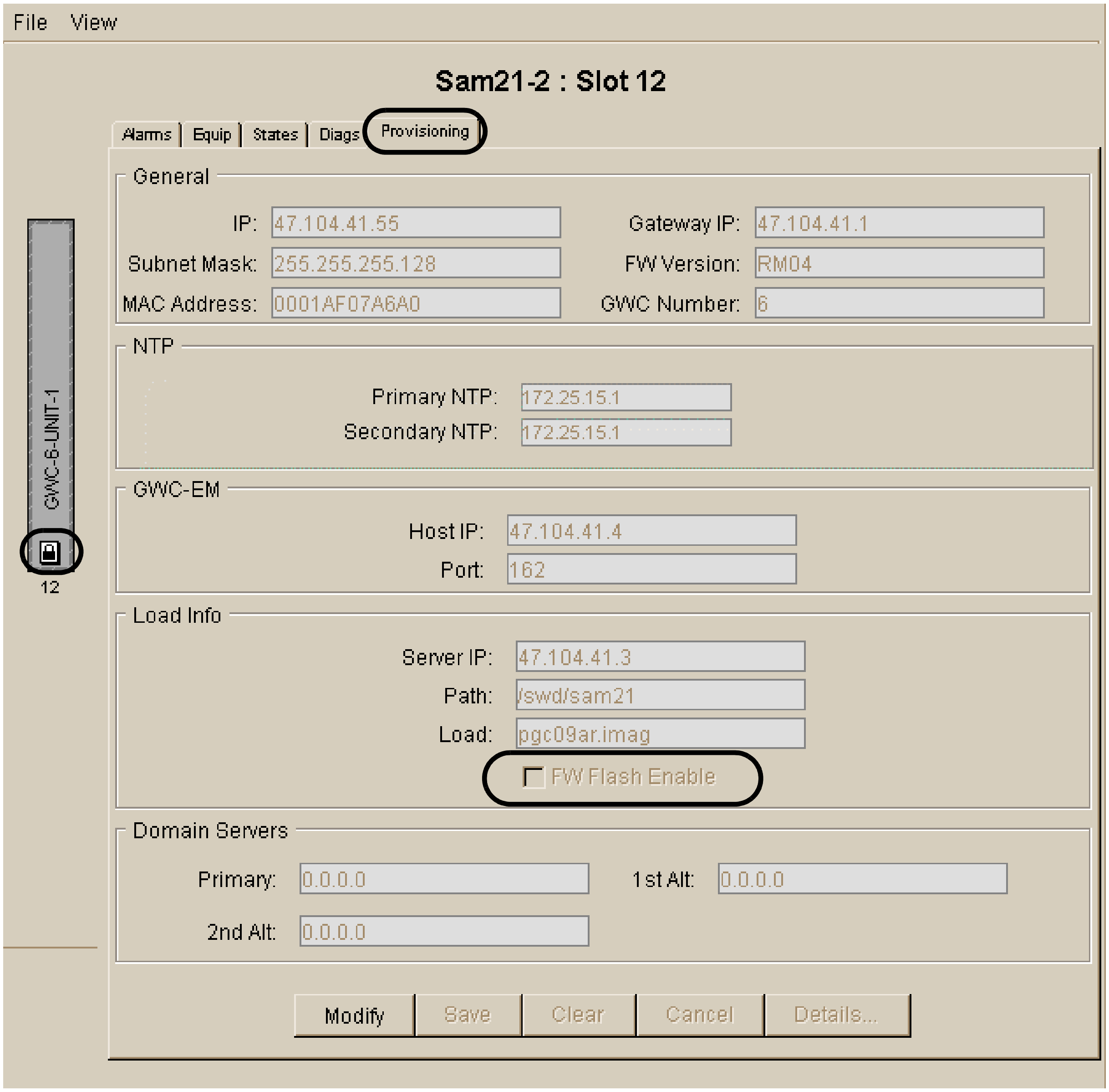
At the CS 2000 SAM21 Manager client

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



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

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



Sam21-2 : Slot 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/sam21

Load: pgc09ar.imag

☐ FW Flash Enable

Domain Servers

Primary: 0.0.0.0

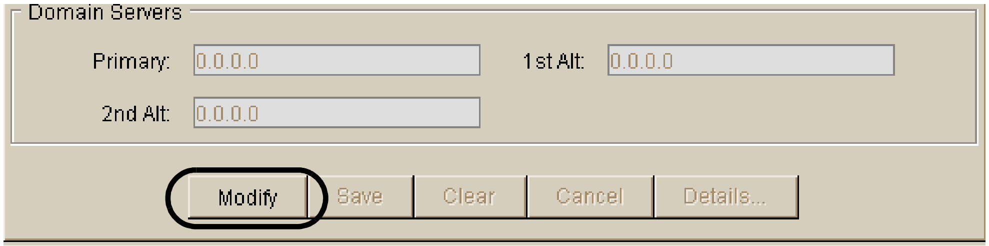
1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

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.

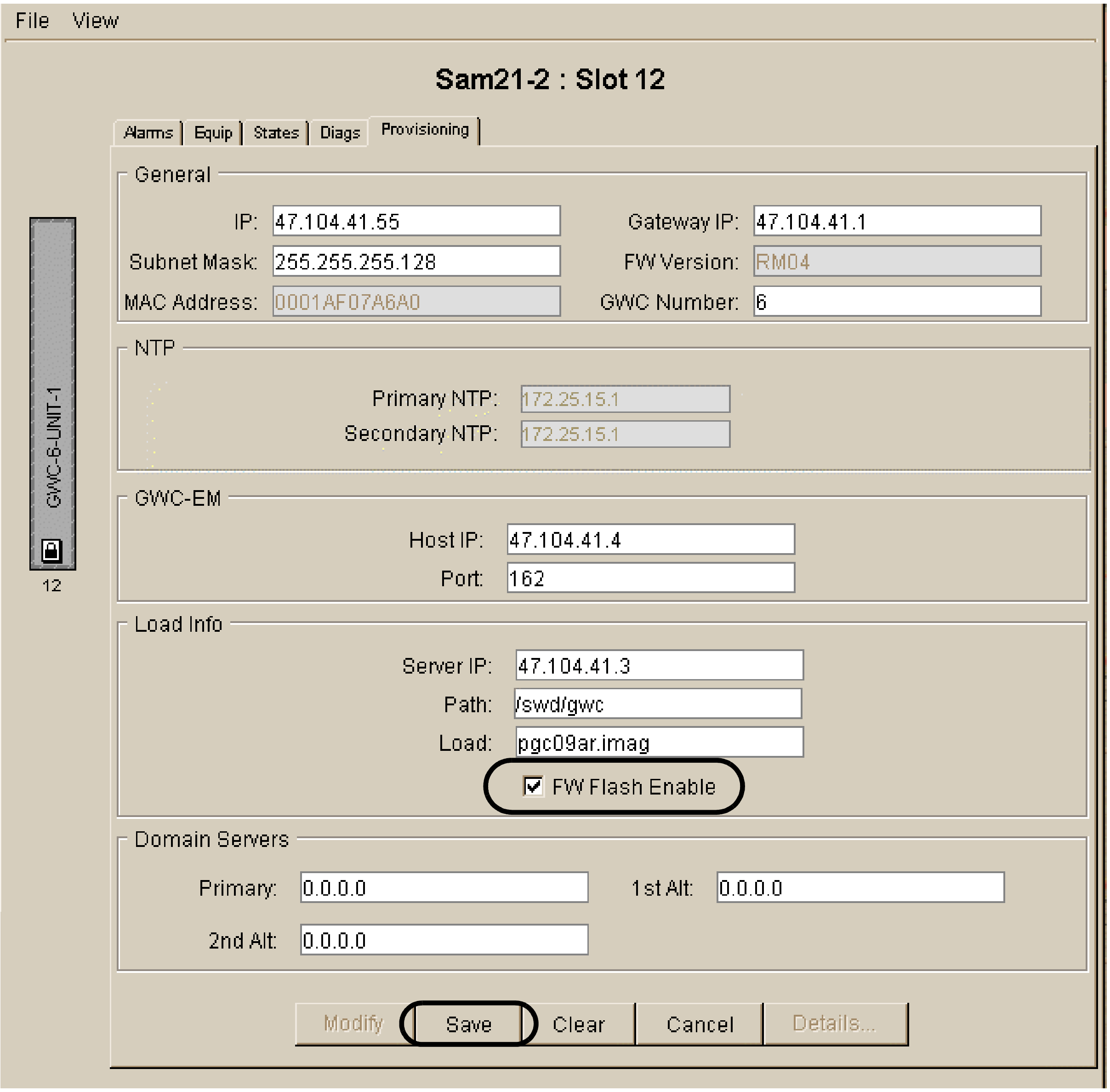


Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

5 Select the “FW Flash Enable” checkbox.



Sam21-2 : Slot 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: pgc09ar.imag

☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

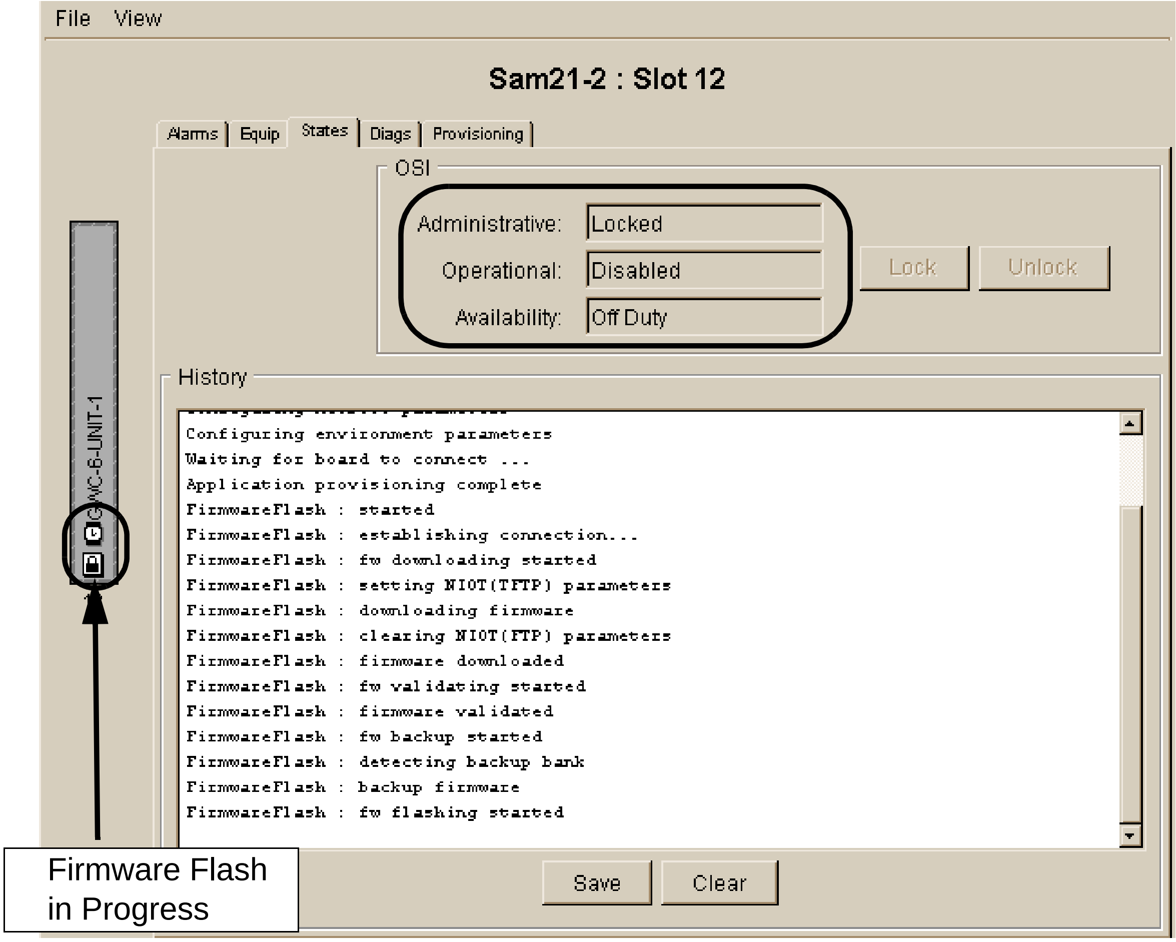
2nd Alt: 0.0.0.0

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.)



Sam21-2 : Slot 12

OSI

Administrative: Locked

Operational: Disabled

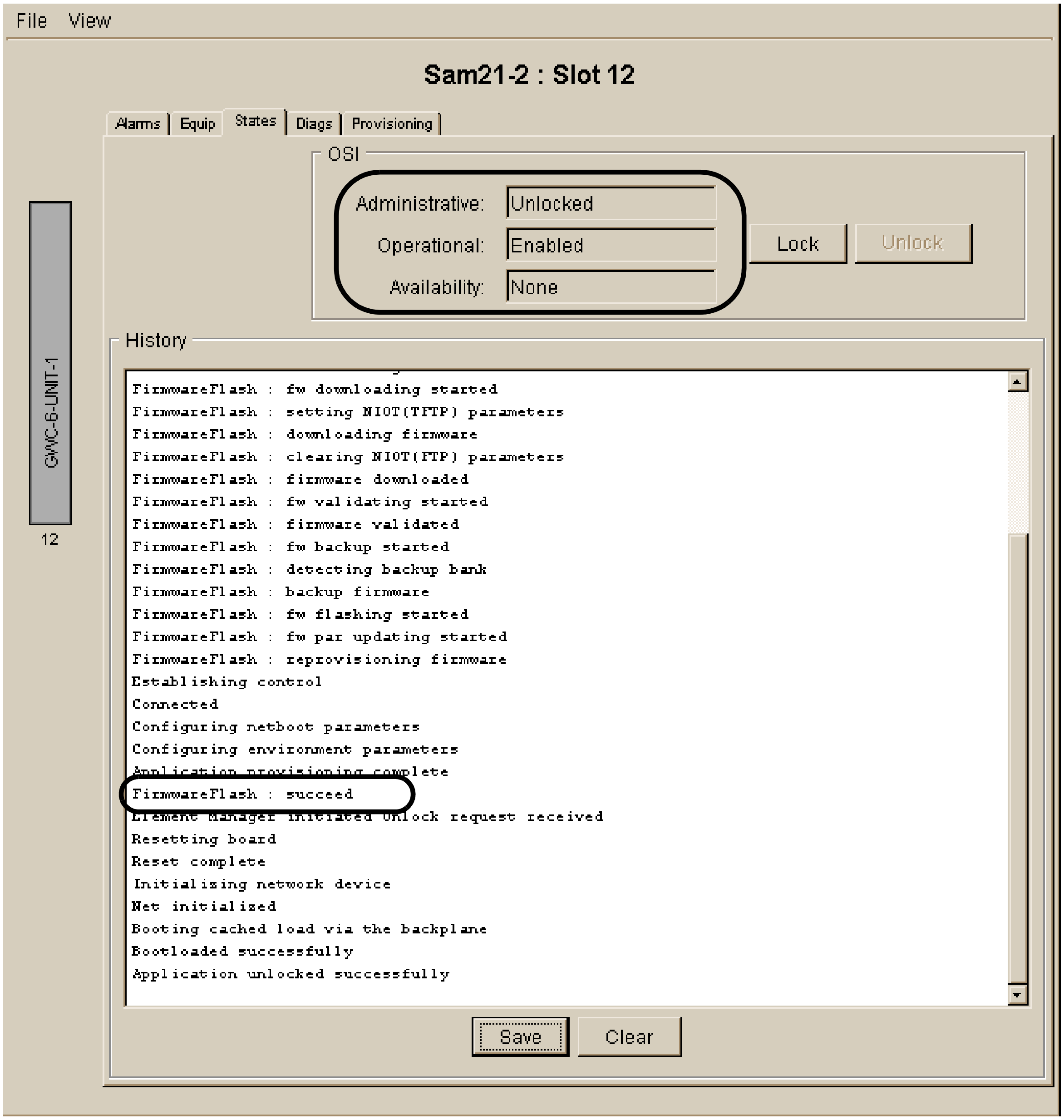
Availability: Off Duty

History

```
Configuring environment parameters
Waiting for board to connect ...
Application provisioning complete
FirmwareFlash : started
FirmwareFlash : establishing connection...
FirmwareFlash : fw downloading started
FirmwareFlash : setting NIOT(TFTP) parameters
FirmwareFlash : downloading firmware
FirmwareFlash : clearing NIOT(FTP) parameters
FirmwareFlash : firmware downloaded
FirmwareFlash : fw validating started
FirmwareFlash : firmware validated
FirmwareFlash : fw backup started
FirmwareFlash : detecting backup bank
FirmwareFlash : backup firmware
FirmwareFlash : fw flashing started
```

Firmware Flash in Progress

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.



Administrative: Unlocked
Operational: Enabled
Availability: None

```
FirmwareFlash : fw downloading started
FirmwareFlash : setting NIOT(TFTP) parameters
FirmwareFlash : downloading firmware
FirmwareFlash : clearing NIOT(FTP) parameters
FirmwareFlash : firmware downloaded
FirmwareFlash : fw validating started
FirmwareFlash : firmware validated
FirmwareFlash : fw backup started
FirmwareFlash : detecting backup bank
FirmwareFlash : backup firmware
FirmwareFlash : fw flashing started
FirmwareFlash : fw par updating started
FirmwareFlash : reprovisioning firmware
Establishing control
Connected
Configuring netboot parameters
Configuring environment parameters
Application provisioning complete
FirmwareFlash : succeed
Element Manager initiated Unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

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

10 The procedure is complete.

Force a firmware flash of a GWC card

Purpose of this procedure

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

> ***Note:*** If you use the procedure Firmware flash a GWC card on page 145 in this NTP, you will not be able to flash a GWC card's firmware if it has the same firmware version as the CS 2000 Core Manager or CBM.

When to use this procedure

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

Prerequisites

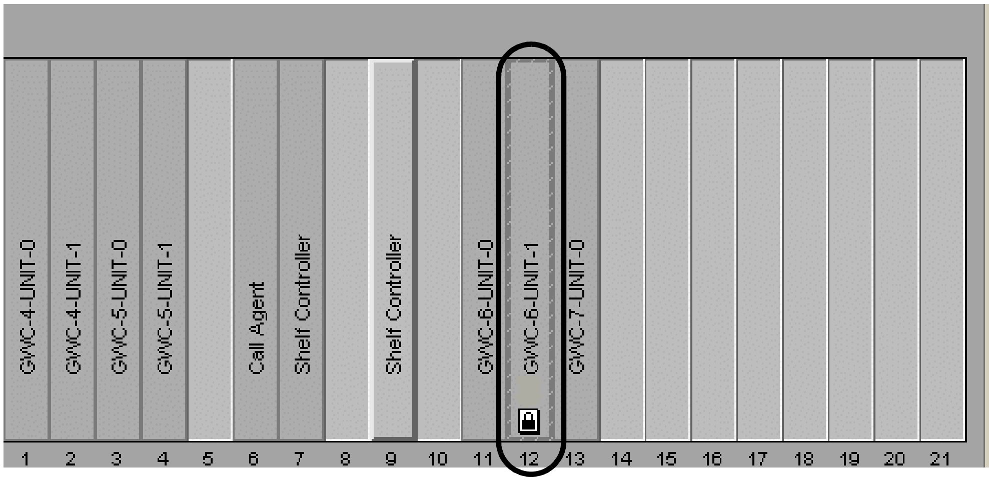
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in the Gateway Controller Security and Administration NTP, NN10213-611.

Action

At the CS 2000 SAM21 Manager client

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

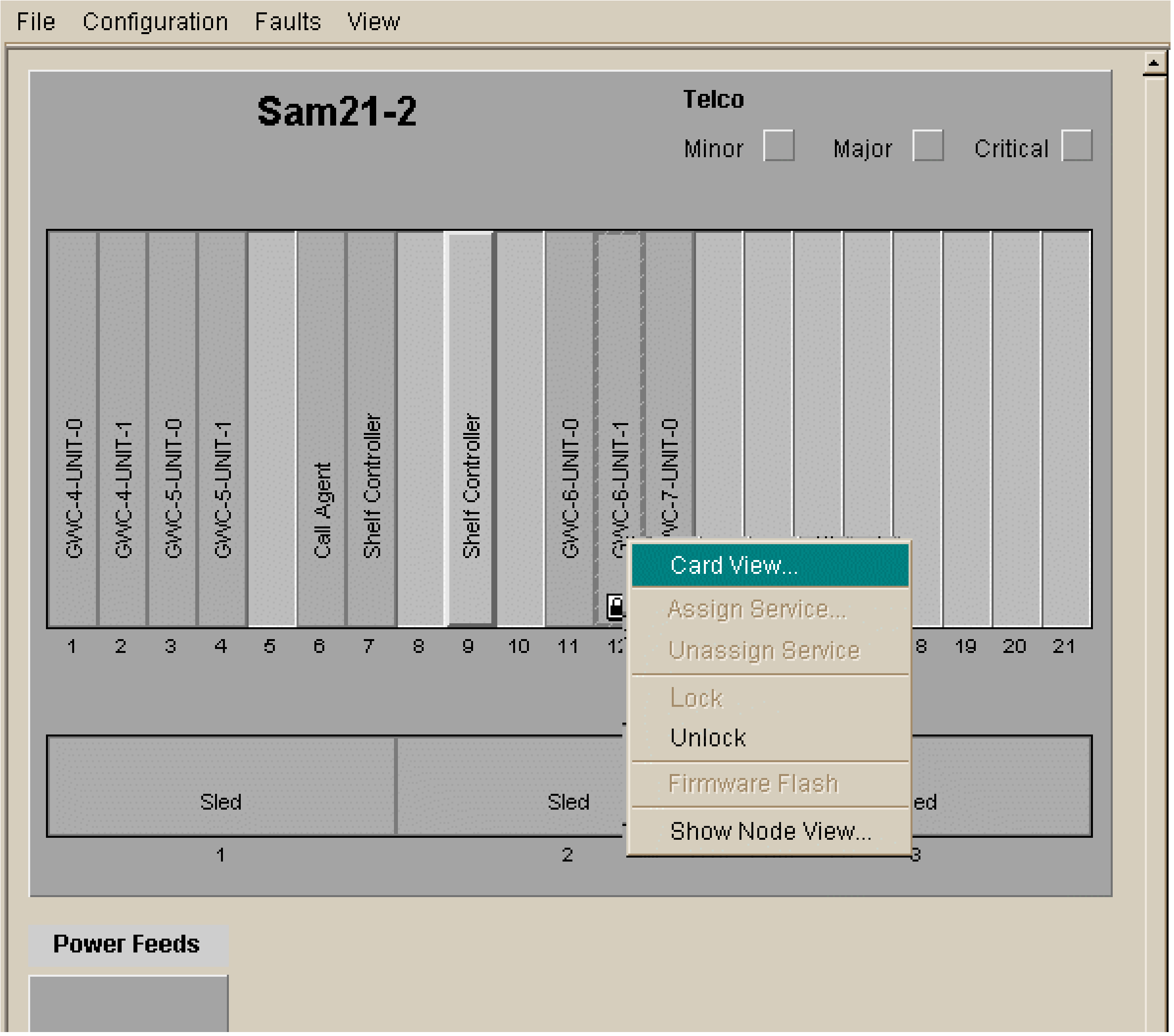
> ***Note:*** If you have just locked the card using the Card View, click on the **View** menu and select **Shelf View**.



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

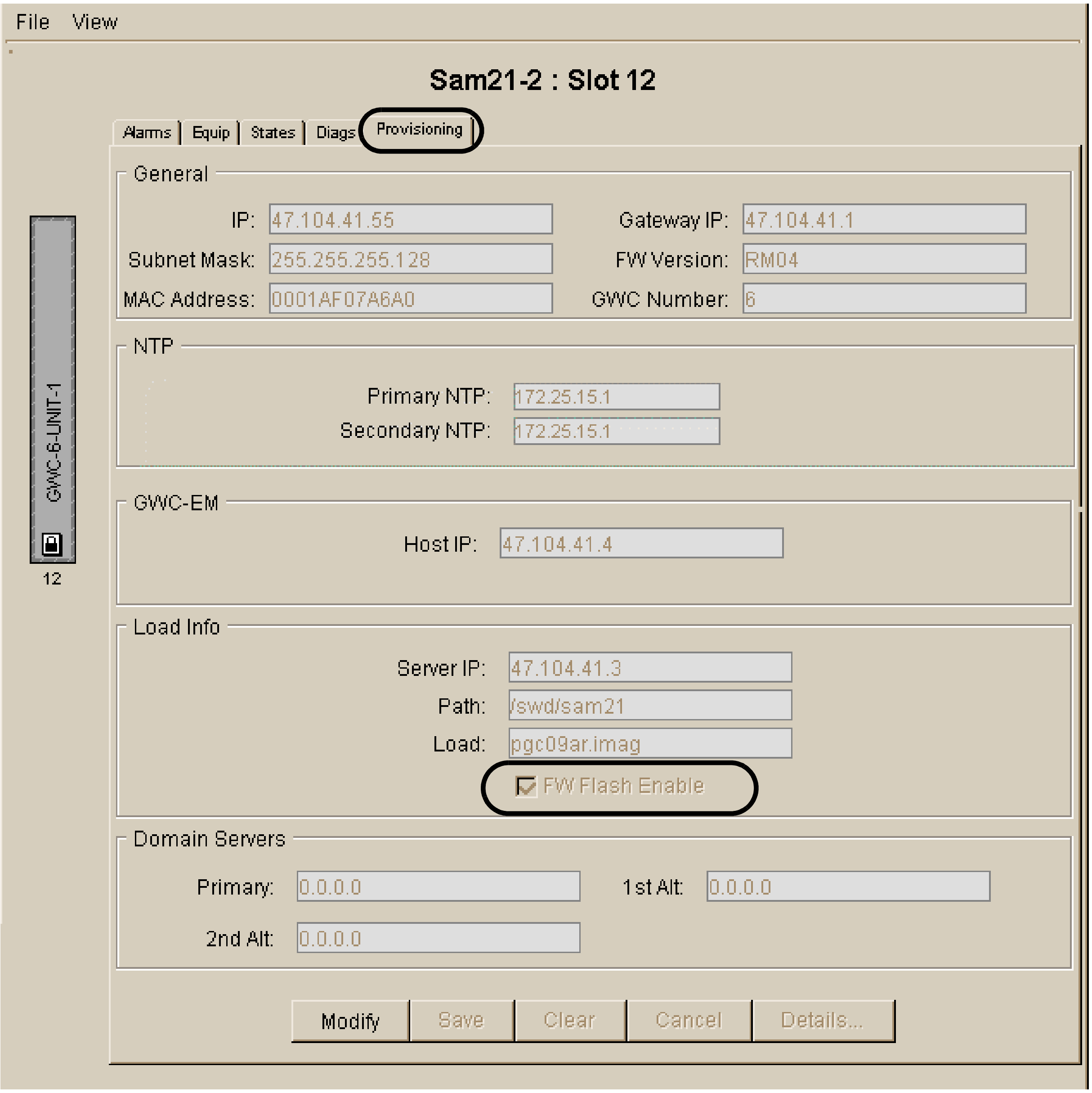
If	Do
If the “Firmware Flash” option is available	skip to step step 8
If the “Firmware Flash” option is not available (the text is faded in the pop-up menu)	go to step 3

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



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

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



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

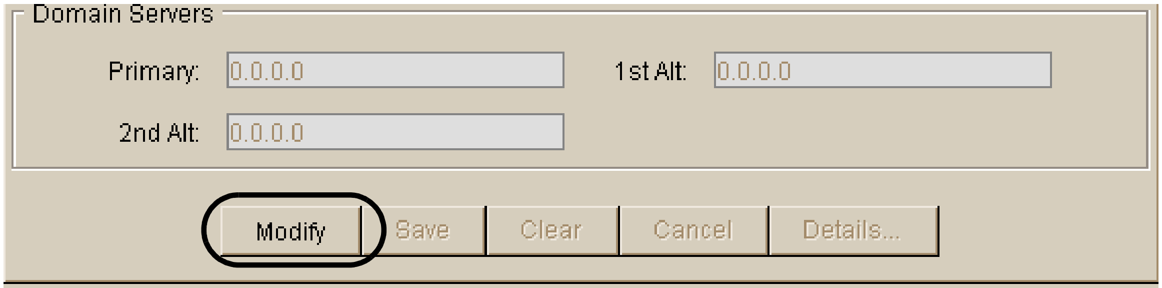
Load Info

Server IP: 47.104.41.3
Path: /swd/sam21
Load: pgc09ar.imag
☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0
1st Alt: 0.0.0.0
2nd Alt: 0.0.0.0

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

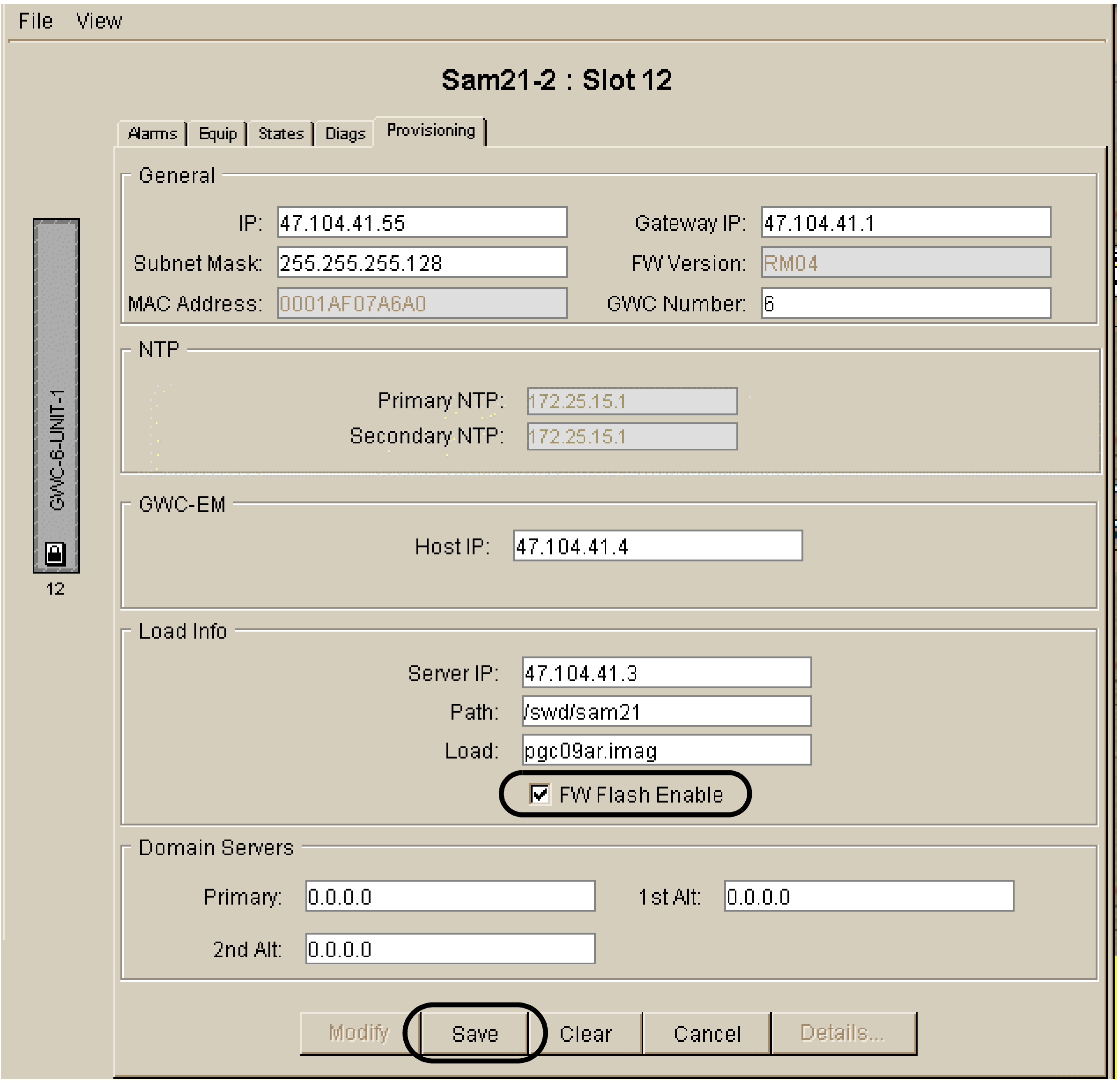


Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

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



Sam21-2 : Slot 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

Load Info

Server IP: 47.104.41.3

Path: /swd/sam21

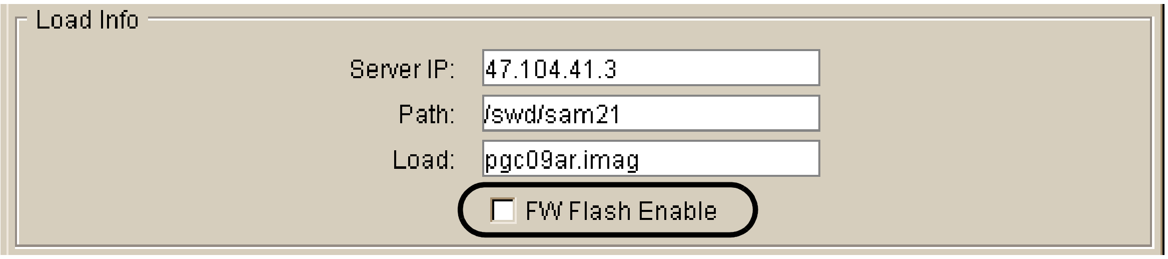
Load: pgc09ar.imag

☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0 1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0



Load Info

Server IP: 47.104.41.3

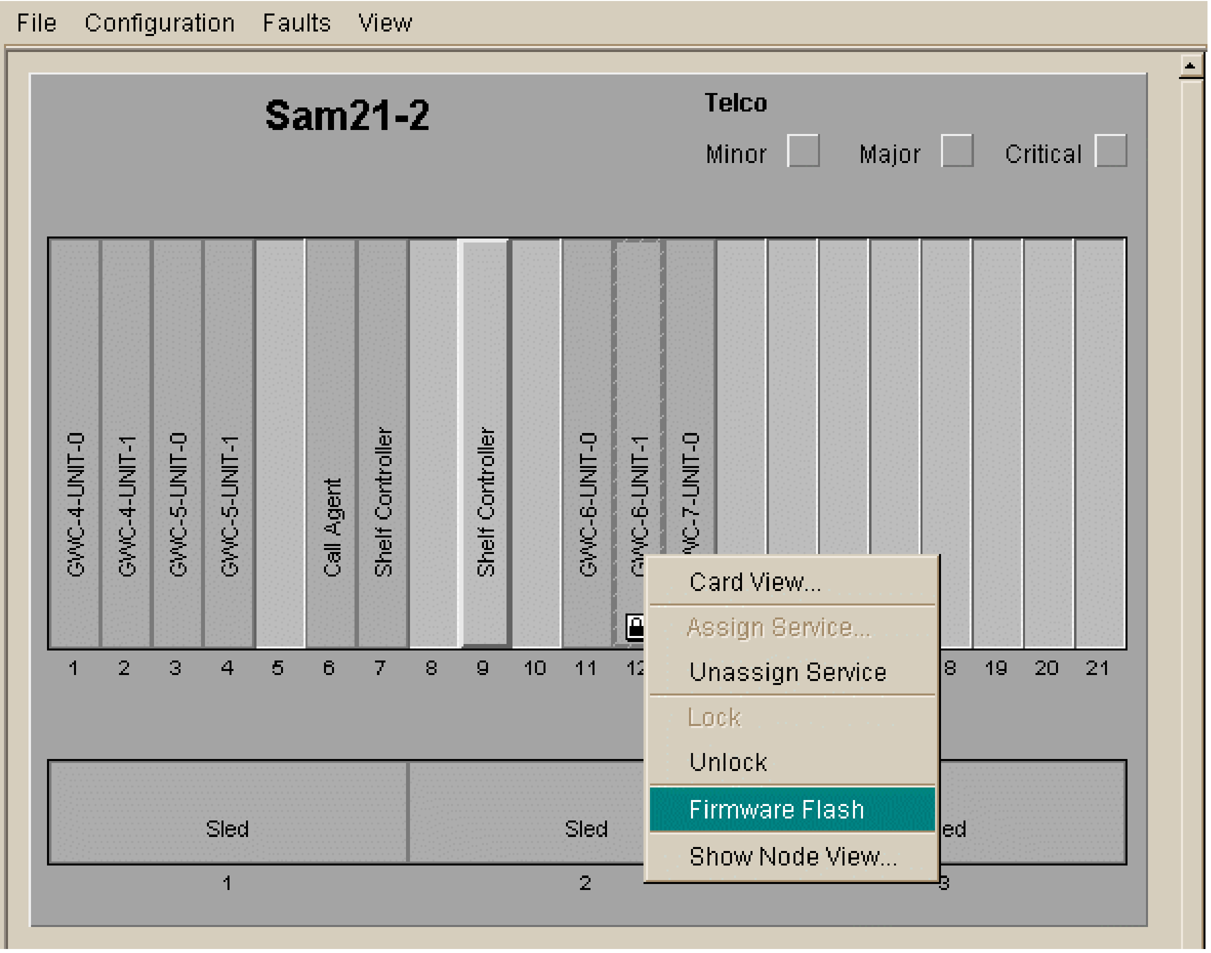
Path: /swd/sam21

Load: pgc09ar.imag

□ FW Flash Enable

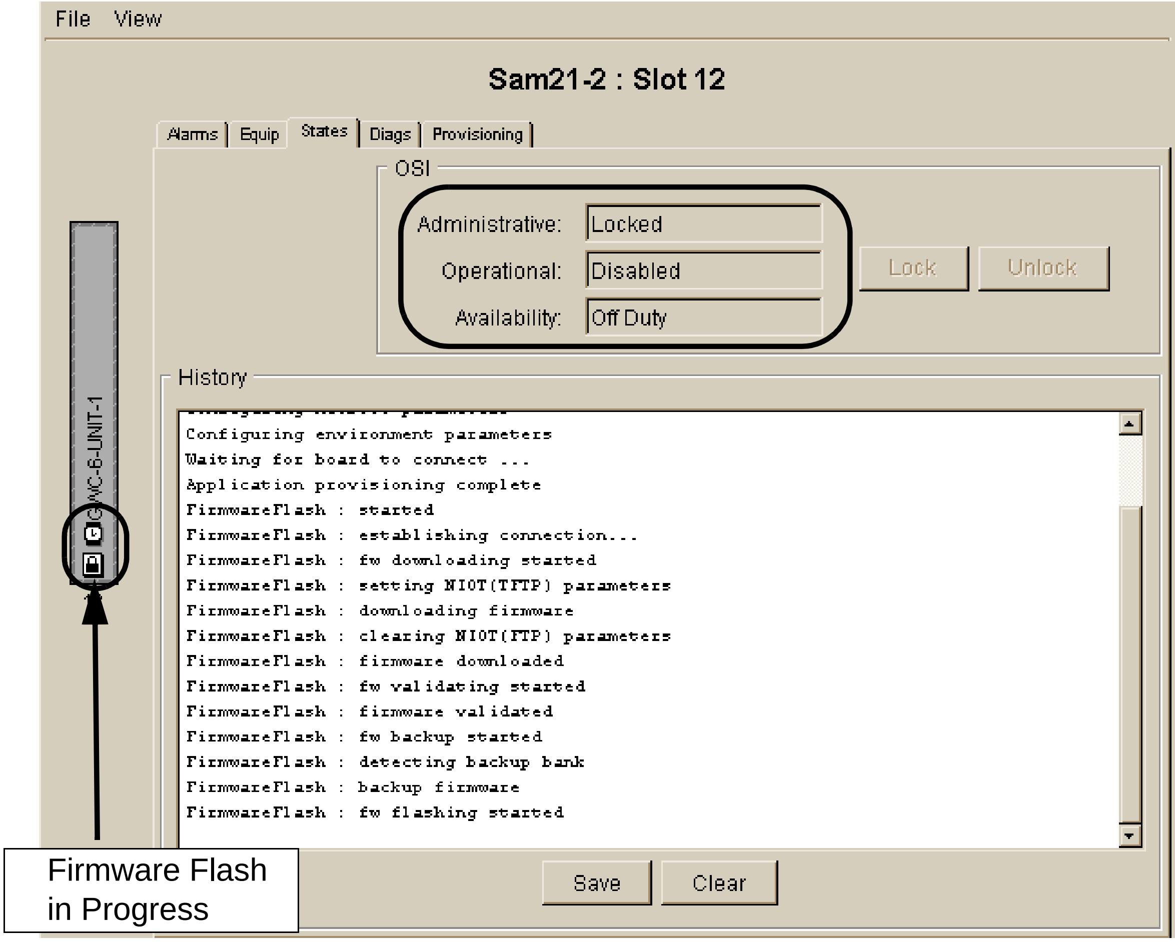
7 Click the **Save** button at the bottom of the screen to save the provisioning change.

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.)



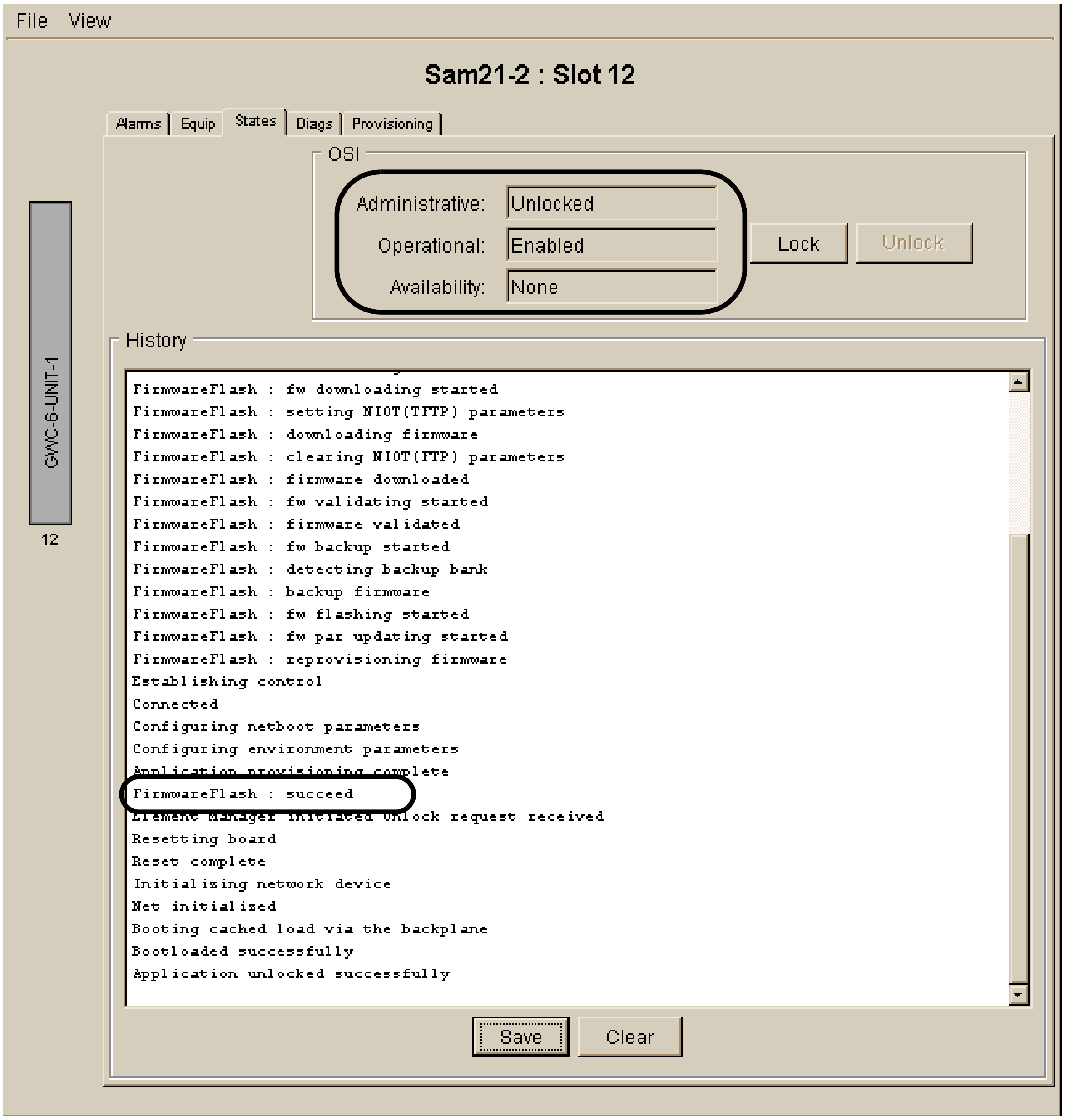
Sam21-2 : Slot 12

Administrative: Locked
Operational: Disabled
Availability: Off Duty

```
Configuring environment parameters
Waiting for board to connect ...
Application provisioning complete
FirmwareFlash : started
FirmwareFlash : establishing connection...
FirmwareFlash : fw downloading started
FirmwareFlash : setting NIOT(TFTP) parameters
FirmwareFlash : downloading firmware
FirmwareFlash : clearing NIOT(FTP) parameters
FirmwareFlash : firmware downloaded
FirmwareFlash : fw validating started
FirmwareFlash : firmware validated
FirmwareFlash : fw backup started
FirmwareFlash : detecting backup bank
FirmwareFlash : backup firmware
FirmwareFlash : fw flashing started
```

Firmware Flash in Progress

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.



Sam21-2 : Slot 12

Administrative: Unlocked

Operational: Enabled

Availability: None

```
FirmwareFlash : fw downloading started
FirmwareFlash : setting NIOT(TFTP) parameters
FirmwareFlash : downloading firmware
FirmwareFlash : clearing NIOT(FTP) parameters
FirmwareFlash : firmware downloaded
FirmwareFlash : fw validating started
FirmwareFlash : firmware validated
FirmwareFlash : fw backup started
FirmwareFlash : detecting backup bank
FirmwareFlash : backup firmware
FirmwareFlash : fw flashing started
FirmwareFlash : fw par updating started
FirmwareFlash : reprovisioning firmware
Establishing control
Connected
Configuring netboot parameters
Configuring environment parameters
Application provisioning complete
FirmwareFlash : succeed
Element manager initiated unlock request received
Resetting board
Reset complete
Initializing network device
Net initialized
Booting cached load via the backplane
Bootloaded successfully
Application unlocked successfully
```

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

12 The 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 (SDM) or Core and Billing Manager (CBM). For more information on GWC software imaging, refer to section GWC software imaging on page 11 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 141 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.

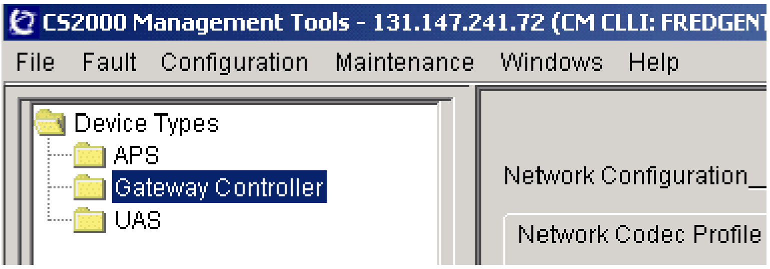
Prerequisites

This procedure has no prerequisites.

Action

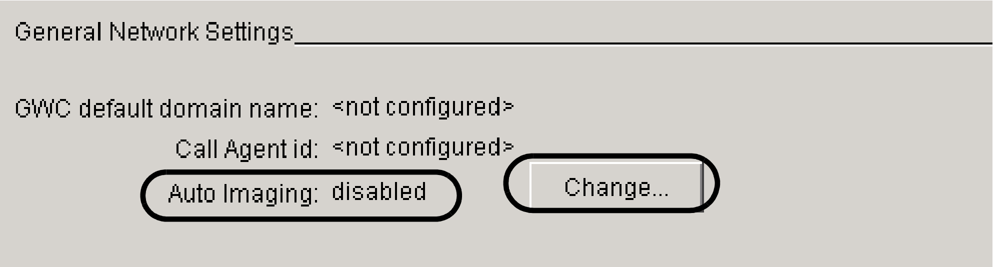
At the CS 2000 GWC Manager client

1 Select Gateway Controller from the Device Types menu.


CS2000 Management Tools - 131.147.241.72 (CM CLLI: FREDGENT
File Fault Configuration Maintenance Windows Help
Device Types
APS
Gateway Controller
UAS
Network Configuration
Network Codec Profile

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”.



General Network Settings

GWC default domain name: <not configured>

Call Agent id: <not configured>

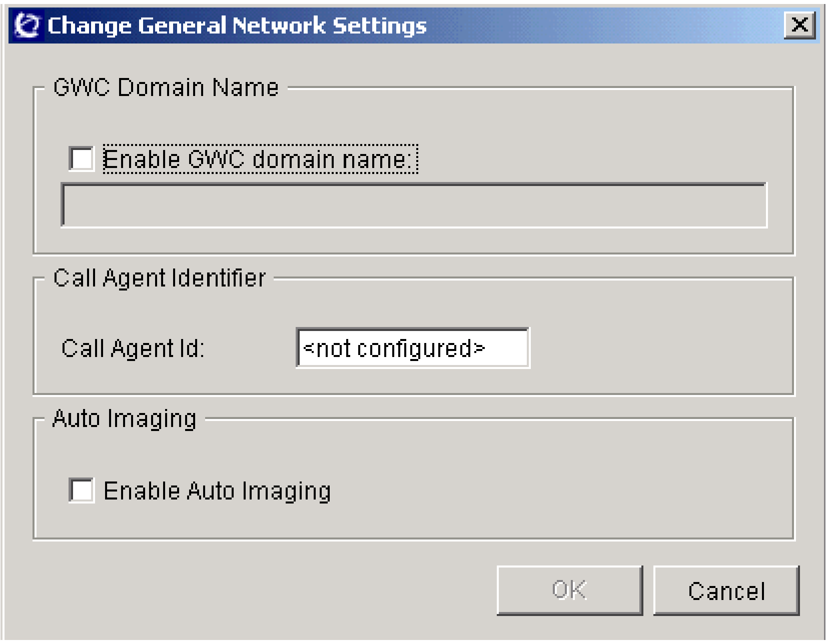
Auto Imaging: disabled

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

- GWC Domain Name - Refer to procedure “Add/change the RMGC default domain” in the Gateway Controller Configuration Management NTP, NN10205-511.
- Call Agent Identifier - Refer to procedure “Set the call agent identifier” in the following locations:
  - — Gateway Controller Configuration Management NTP, NN10205-511
  - — Solutions Upgrades NTP, NN10261-450 (ATM) or NN10344-450 (IP)

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

The Change General Network Settings dialog box is displayed.



Change General Network Settings

GWC Domain Name

□ Enable GWC domain name:

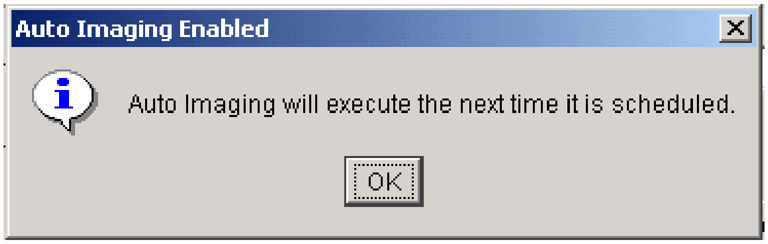
Call Agent Identifier

Call Agent Id: <not configured>

Auto Imaging

□ Enable Auto Imaging

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



Auto Imaging Enabled

Auto Imaging will execute the next time it is scheduled.

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 The 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.

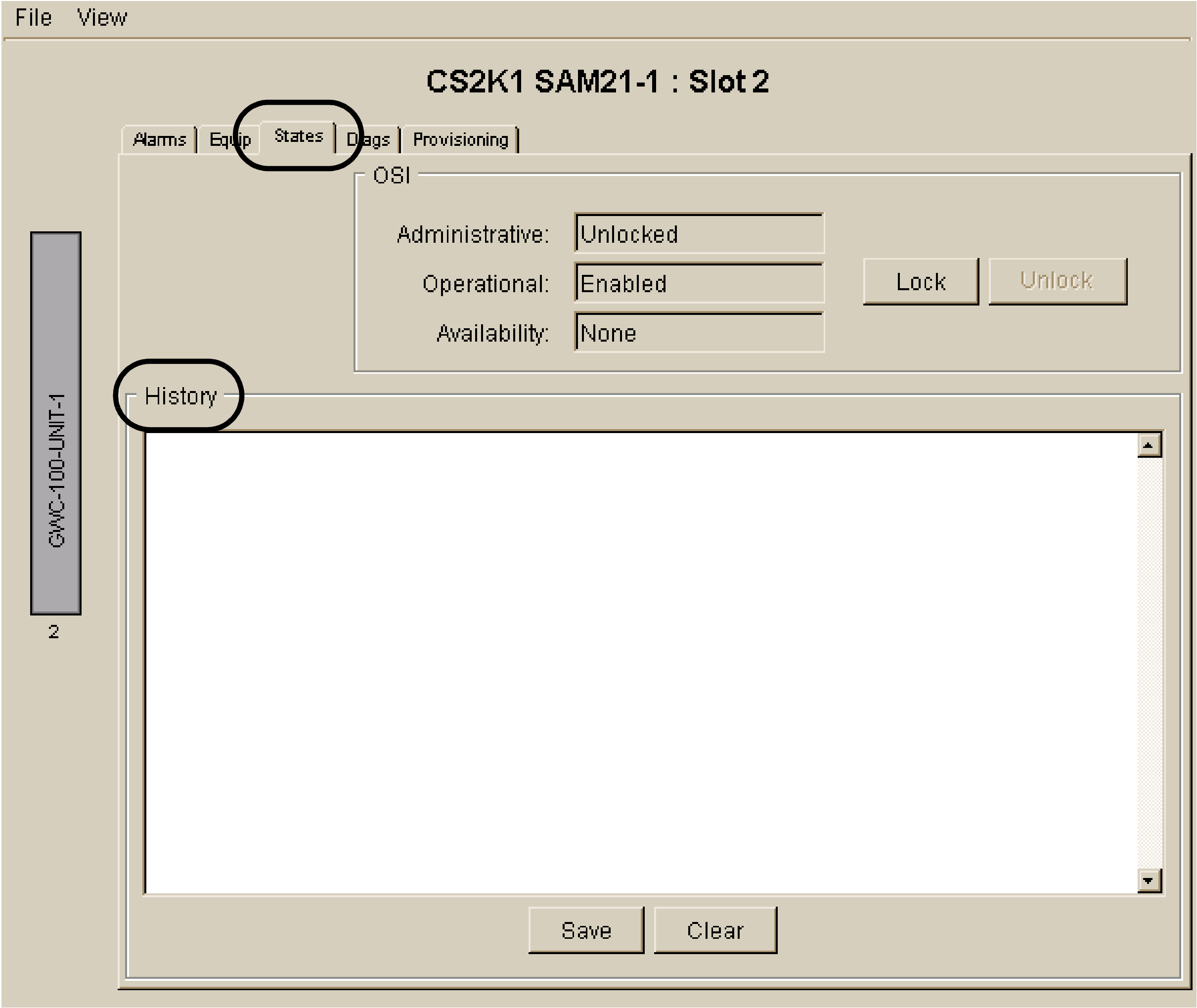
GWC does not RTS

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 165.

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 166.

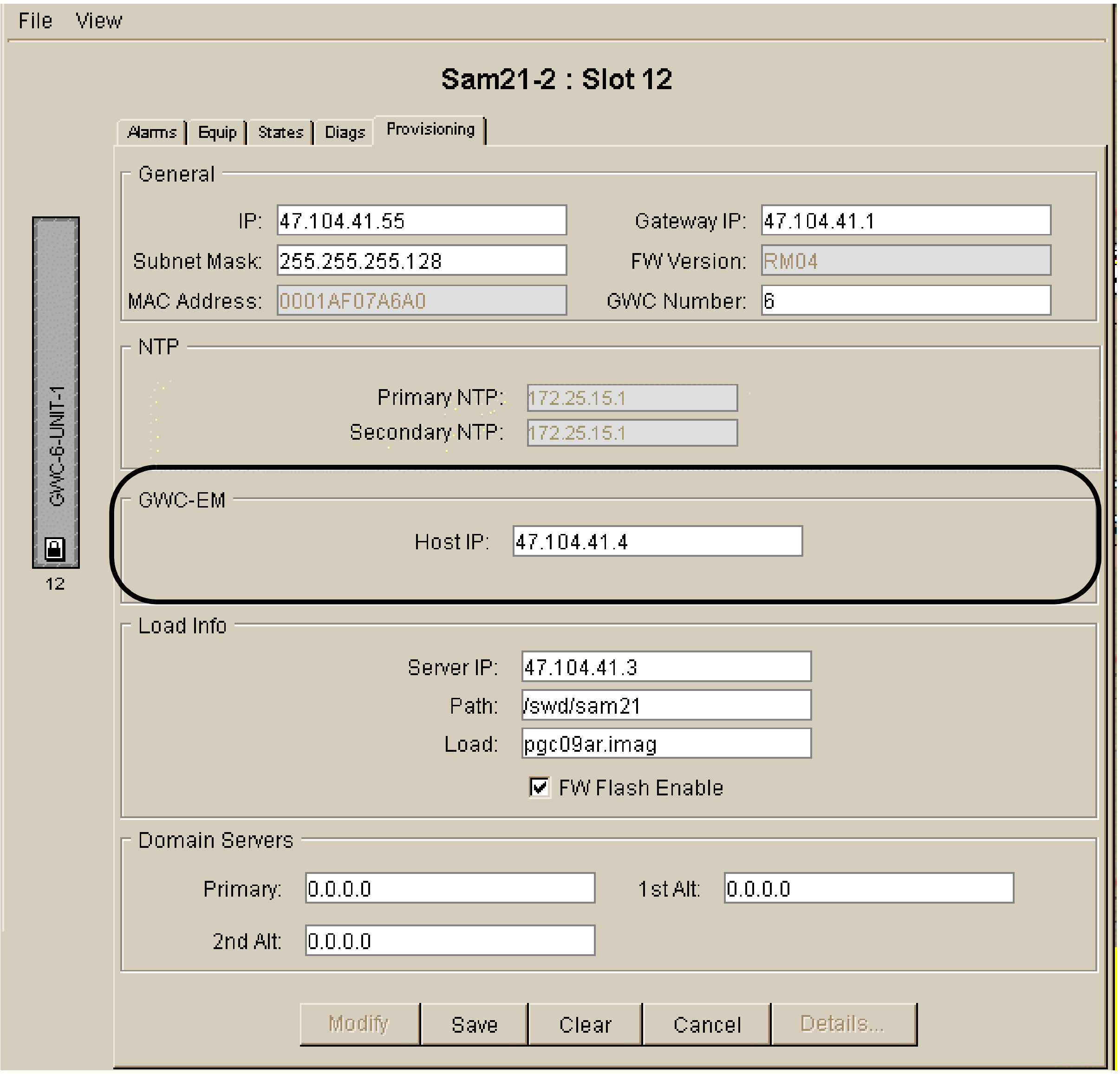


Administrative: Unlocked

Operational: Enabled

Availability: None

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.



Sam21-2 : Slot 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

Load Info

Server IP: 47.104.41.3
Path: /swd/sam21
Load: pgc09ar.imag
☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0
1st Alt: 0.0.0.0
2nd Alt: 0.0.0.0

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 162.

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.

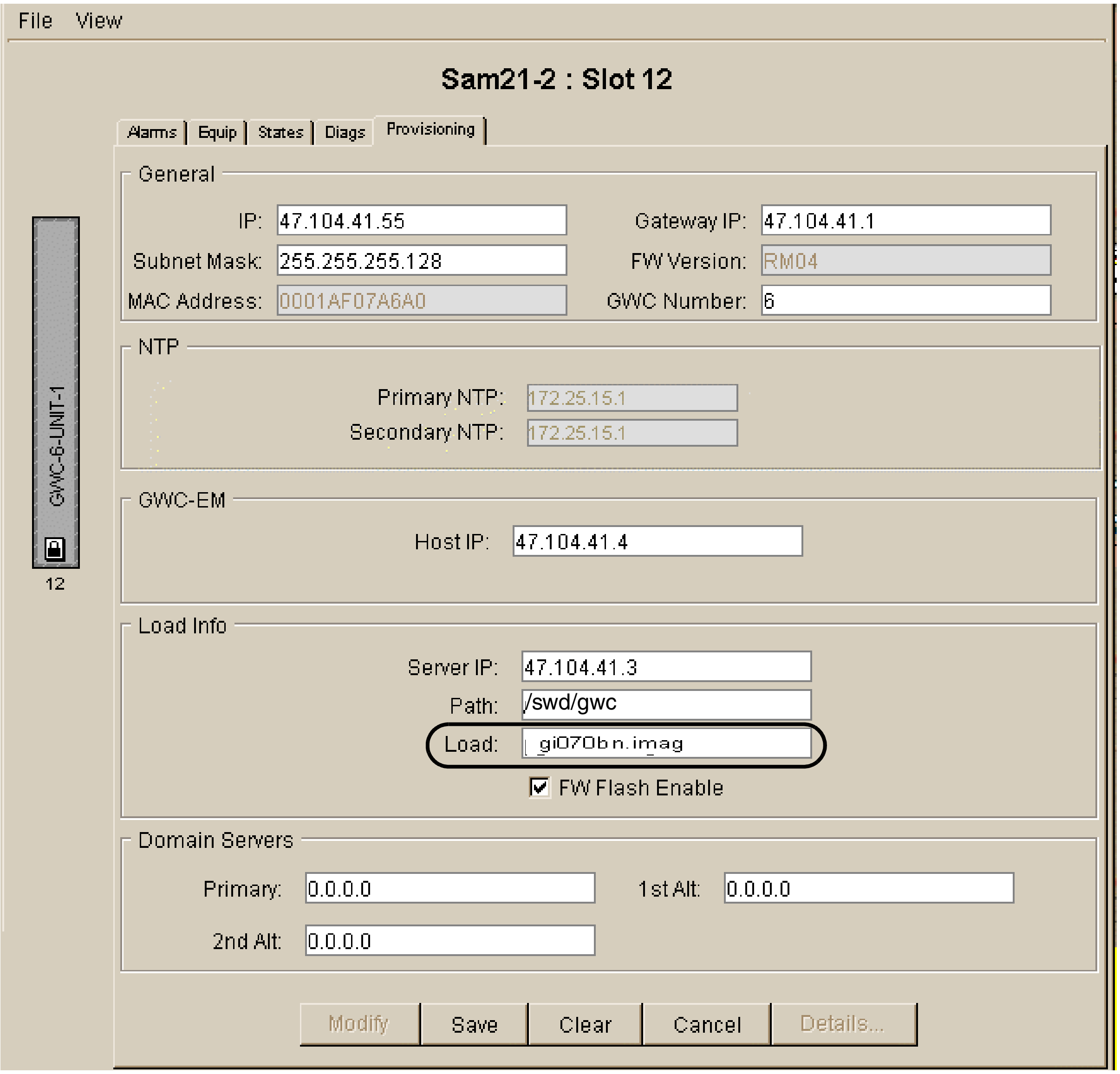
At the CS 2000 SAM21 Manager client

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 (SDM) or Core and Billing Manager (CBM). Also, verify that the file's permissions are set to 755.



Sam21-2 : Slot 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

Load Info

Server IP: 47.104.41.3

Path: /swd/gwc

Load: gi070bn.imag

☑ FW Flash Enable

Domain Servers

Primary: 0.0.0.0

1st Alt: 0.0.0.0

2nd Alt: 0.0.0.0

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 169.

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 the Gateway Controller Configuration Management NTP, 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.