Nortel Gateway Controller Upgrades and Patches

This chapter describes how to upgrade the software on the Gateway Controller (GWC).

New in this release

This section describes changes in GWC upgrades in (I)SN09FF.

Feature changes

None

Other changes

This release introduces the following additional changes to GWC upgrades:

- new high-level procedures to improve usability of detailed GWC upgrade procedures and simplify the GWC upgrade process

Upgrade paths

Nortel Networks supports the following upgrade paths:

- (I)SN08 to (I)SN09FF
- (I)SN09 to (I)SN09FF

Impacts of an upgrade

This section provides the following information:

- the estimated time to complete a software upgrade
- the service impacts of a software upgrade
- other information affecting a software upgrade

Time to complete an upgrade

The following table lists the tasks to upgrade the software on a Gateway Controller node and the estimated time to complete each task.

Table 1 Estimated time to complete a software upgrade

Task	Time
Preparing for the upgrade	45 minutes
Upgrading the software	18 to 24 minutes per node
Completing the upgrade	15 minutes to 1 hour
Total estimated upgrade time	2 hours 10 minutes

Note: The condition of the office before the upgrade may require additional traffic analysis and log monitoring after the upgrade.

Service impacts

CAUTION
Loss of service
Service outages occur during the upgrade of Gateway Controller software.

The upgrade of Gateway Controller software creates the following service impacts:

- Stable two-port calls survive a switch of activity between the GWC nodes. However, calls in setup mode during the SWACT are dropped.
- The following table lists possible call service impacts for the GWC card types during the following scenarios:
  - an upgrade from one release to a newer release
  - an maintenance upgrade to a newer version of the same release
  - a downgrade from one release to a previous release

Table 2 GWC upgrade call service impacts (Sheet 1 of 2)

GWC Type	Upgrade	Maintenance	Downgrade
AUDCNTL	Stable announcement and conference calls survive.	Stable announcement and conference calls survive.	Stable announcement and conference calls not using new features survive.
VRDN	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	Calls not using new features survive.
SIP-T	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	NO calls survive.

Table 2 GWC upgrade call service impacts (Sheet 2 of 2)

GWC Type	Upgrade	Maintenance	Downgrade
MG 15000 trunk	All stable calls survive. Transient calls (ringing, dialing, clearing) are not guaranteed to survive.	ALL calls survive.	NO calls 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.

Additional information

Starting in (I)SN08, the Upgrade Automation Tool supports parallel Gateway Controller upgrades.

CS 2000 Management Tools generates new middlebox IDs for network address translator (NAT) devices and policy enforcement point (PEP) servers if these items were provisioned before the upgrade.

System capacity

The software upgrade procedure can impact the system capacity. This means that additional disk space on the OAMP workstation is required for converting existing databases.

System performance

You must perform software upgrade procedures during maintenance periods, as network capacity is reduced during the software upgrade

System limitations during upgrade

During a software upgrade, the system prohibits the following actions:

- System administration
  - adding, deleting, or modifying users
  - setting the time of day
  - changing passwords
- System management
  - modifying the system name
  - adding or deleting system nodes
  - modifying the IP addresses
- Once ethics 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.

Upgrade order for GWC card types

Upgrade GWC card pairs in order based on the type of GWC card. If you use the GWC Upgrade Tool, the tool automatically upgrades the card types in the correct order. If you do not use the GWC Upgrade Tool, you must identify the GWC card types in your office and schedule the upgrades in the correct order.

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

The following table lists the upgrade order for all available GWC card types.

Note: The table lists all available GWC card types. Your office will not have all the card types listed in the table. Refer to the *Gateway*

Controller Basics, NN10189-111, for details on the card types listed in this table and supported in your release.

GWC card type upgrade order

Order	GWC card type
1	AC
2	BICC - Long Distance Voice over IP (UA-AAL1) solutions only
3	VRDN - see Note 1
4	Session Server - see Note 2 and Note 3
5	SIP-T/APG/RA - see Note 4
6	APG/RA - see Note 4
7	SIP-T/APG - see Note 4
8	APG - see Note 4
9	SIP-T
10	Trunk
11	H.323
12	V5.2 trunk
13	Lines - includes Centrex IP Client Manager (CICM)

Note 1: After upgrading the VRDN GWC to SN09FF, for each MCS gateway whose gateway host points to this CS 2000, you must change the gateway type to 'CS2K SN09FF VRDN' using the corresponding MCS provisioning client (see procedure GWC provisioning in MCS in this NTP. Failure to do so may result in certain MCS call scenarios not working properly. For detailed instructions for using the MCS provisioning client, refer to *Provisioning Client User Guide*, NN10043-113.

Note 2: After upgrading the Session Server GWC to SN09FF, for each MCS gateway whose gateway host points to this CS 2000, you must change the gateway type to 'CS2K SN09FF NGSS' using the corresponding MCS provisioning client (see procedure GWC provisioning in MCS in this NTP). Failure to do so may result in certain MCS call scenarios not working properly. For detailed

instructions for using the MCS provisioning client, refer to *Provisioning Client User Guide*, NN10043-113.

Note 3: The Session Server-Trunks (SS-T) was a new component in SN07. It can replace the Virtual Routing Destination Node (VRDN) GWC as a SIP-T interface. The following office configurations are supported in SN07: SS only, VRDN SIP-T only, or VRDN SIP-T and SS-T co-existing in the same office.

Note 4: The APG functionality was removed in the SN07 release. All GWC service profiles that were required to support the APG functionality (all profiles with APG in their names, such as, SIP_T_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. It is recommended that the existing DPT GWCs that still use these profiles migrate to SIP-T or SIP_TINTL profile to optimize resource utilization (resources previously reserved for APG are released for other tasks). The Packet Media Anchor (in IP network solutions) is the replacement device for the APG functionality.

Note 5: The manual upgrade process does not support parallel upgrades. While it is possible to save time by loading all GWC card pairs of a given GWC type and performing all the SwActs at the same time, this is not recommended or supported for a live office upgrade as it would cause an out of service condition for all GWC nodes.

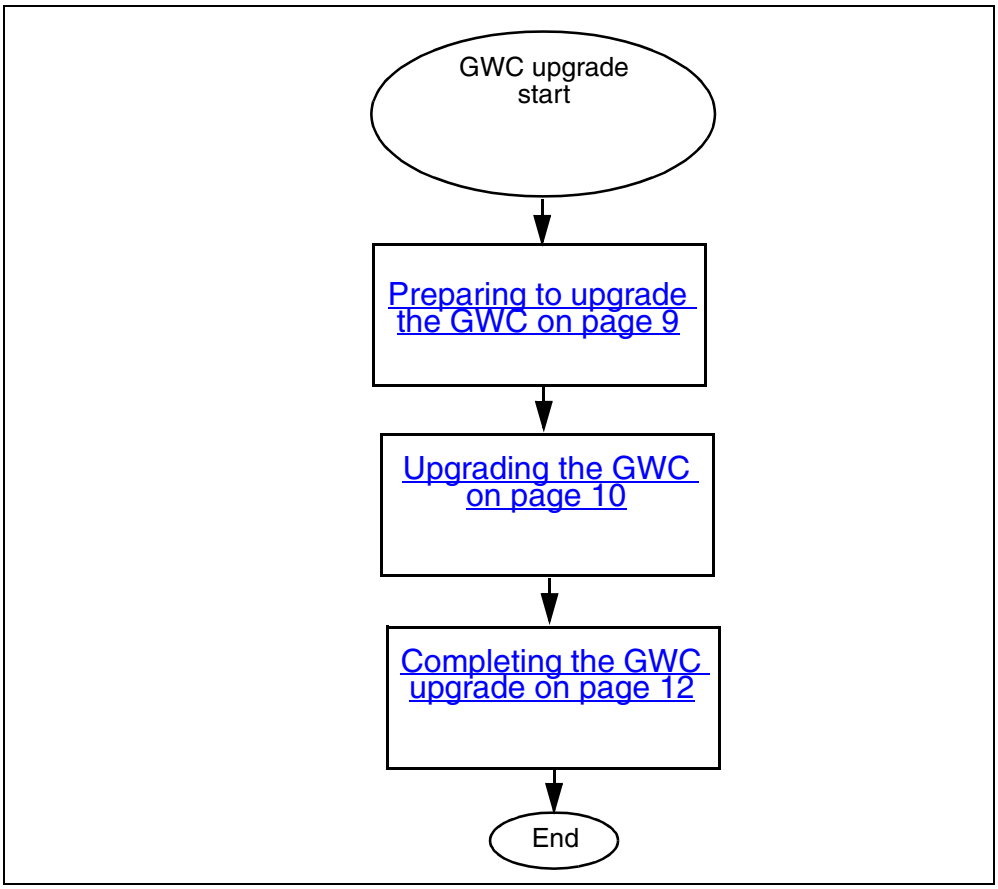
Note 6: Starting in SN06, the Redirecting Media Gateway Controller (RMGC) application migrates from the CS 2000 Management Tools server to the GWC platform. RMGC service cannot be provided between upgrading the CS 2000 Management Tools server and commissioning the GWC-based RMGC service.

It is assumed that an existing Audio Controller GWC is used to host the RMGC application. If commissioning a new GWC for RMGC in SN09FF, refer to appropriate procedures in *Gateway Controller Configuration Management*, NN10205-511.

GWC upgrade tasks

This taskflow shows you the sequence of tasks you perform to upgrade this component.

Figure 1 GWC upgrade tasks



Preparing to upgrade the GWC

The following procedure provides the steps you need to execute prior to upgrading the GWC. When applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

This procedure has no prerequisites.

Action

Perform the following procedures:

1. Transfer the new software to the boot server for your GWC.
    - If you are using a load delivered on CD, perform Copying GWC software from CD to the boot server on page 110
    - If you are using a load delivered though Electronic Software Delivery (ESD), perform the following procedures:
        - — Transferring and mounting an ISO image on an SPFS-based server on page 13
        - — Copying GWC software from an SFPS-based server to the boot server on page 33

After you have performed these procedures, go toUpgrading the GWC on page 10.

Upgrading the GWC

The following procedure provides the steps you need to execute to upgrade the GWC. When applicable, a reference to the procedure that contains the detailed steps is provided.

Prerequisites

This procedure has the following prerequisites:

- You have completed procedure Preparing to upgrade the GWC on page 9.
- Your office has the following patch audit tools:
  - — Pre Upgrade Patch Calculator (if loads are delivered on CD)
  - — Patch Audit for Inform Lists

  Patch audit tools are available at www.nortel.com.
- Make sure your current GWC software is patch current.

Action

Perform the following procedures

1. Identify and download any Released (R) and Propogated (P) patches for the new release.
   - If your new GWC software is delivered on CD, perform the following procedures.
     - — Use the Pre Upgrade Patch Calculator Tool and download any patches to your site.
     - — Transferring patches delivered on CD to the NPM database on page 115.
   - If your new GWC software is delivered through ESD, perform Transferring patches delivered through ESD to the NPM database on page 119.
2. Backup your existing GWC software. Perform Create a backup of the GWC load file on page 124.
3. Identify and download any Verification (V) patches for the new release. Repeat the patch download procedures performed earlier and download the patches to the NPM database.
4. Determine if the new load image contains any patches. Perform View the contents of a load file image on page 126. If the new load image contains patches, repeat the patch download procedure you performed earlier and download the patches to the NPM database.

5. Upgrade the GWC software. Perform Upgrade the GWC using the GWC Upgrade Tool on page 37.

   Note: If you wish to perform a manual upgrade, perform Upgrade a standby GWC card software load on page 130

6. If you upgraded a VRDN GWC or Session Server GWC, and your office interworks with an MCS gateway, change the GWC settings in the MCS Manager. Perform GWC provisioning on MCS on page 104.
7. You have upgraded the software on the GWC. Go to Completing the GWC upgrade on page 12.

Completing the GWC upgrade

The following procedure provides the high-level steps to complete the component upgrade. Where applicable, a reference to the step-by-step procedure is provided.

Prerequisites

You have completed procedure Upgrading the GWC on page 10

Action

Perform the following procedures:

- Make sure the correct load name for each Gateway Controller appears in the CS 2000 Management Tools application. Perform Confirming Gateway Controller loads after an upgrade on page 188.

You have completed the upgrade of the Gateway Controller. Continue with the next component to the upgraded.

Transferring and mounting an ISO image on an SPFS-based server

Application

Use this procedure to perform the following tasks:

- uncompress the load on your ESD load repository server
- transfer an uncompressed iso image file from your ESD load repository server to the SPFS-based server
- mount the image on the SPFS-based server

Nortel delivers compressed software loads through Electronic Software Delivery (ESD) to a local load repository server. Once the loads are uncompressed, they are then available as International Standard of Organization (ISO) 9660-compliant images for transfer to an SPFS-based server. A patch ISO image file will be included with the software load.

Prerequisites

This procedure has the following prerequisites:

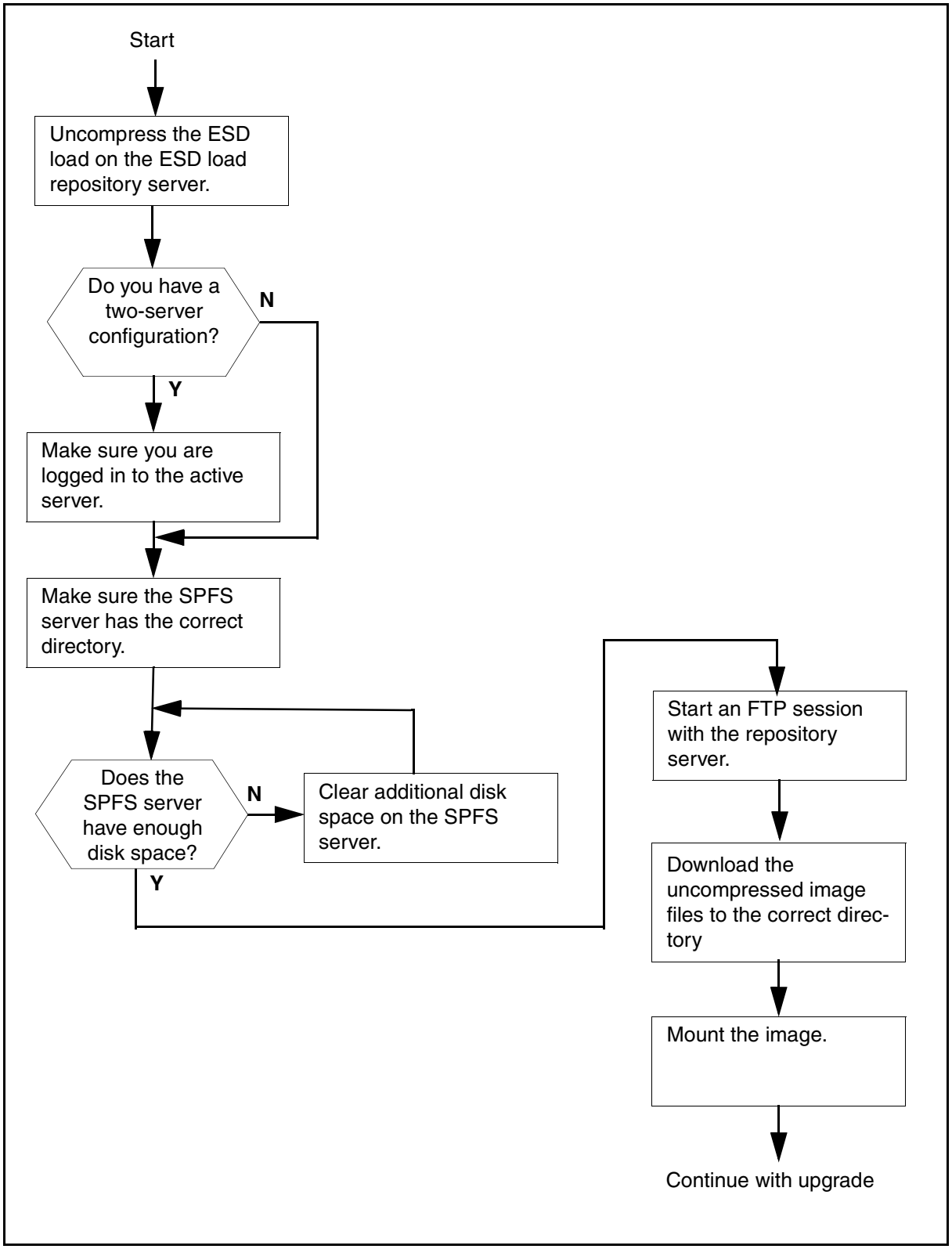
- The ESD load must be available on your ESD load repository server.
- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SPFS-based server.
- You must know the root password to the SPFS-based server.

This procedure requires you to confirm the availability of disk space on the SPFS-based server. If the server does not have the required amount of available disk space, follow your local office policy to clear space. If you do not know your policy or cannot clear the required amount of available disk space, contact your next level of support.

Action

Use the flowchart as an overview of the tasks required to complete this procedure. Use the step-by-step instructions to complete the procedure.

Overview of steps to transfer and mount an ISO image to an SPFS-based server



Uncompressing the load on the ESD load repository server

At the ESD load repository server

1 Log in to the ESD load repository server, and change directory to the drop box location.

Note: Ensure you log in with a user ID that has permission to uncompress files.

2 List the contents of the drop box by typing

```
ls *.gz
```

and pressing the Enter key.

3 Locate the file you want to uncompress.

4 Uncompress the file by typing

```
gzip -d <esd_filename>.tar.gz
```

and pressing the Enter key.

where

esd_filename
is the name of the ESD software load, for example SPFS009F.9F.R.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

5 List the uncompressed file by typing

```
ls *.tar
```

and pressing the Enter key.

Example response

```
SPFS0091.91.R.NCL.NAP.VAULT.1.D.tar
```

6 Unpack the file by typing

```
tar -xvf <esd_filename>.tar
```

and pressing the Enter key.

where

esd_filename
is the name of the ESD software load, for example SPFS009F.9F.R.NCL.NAP.VAULT.1.D, which is the esd_filename for SPFS

The unpacked file is a directory, for example, SPFS009F.9F.R.NCL.NAP.VAULT.1.D, that contains the iso image files.

7 Access this directory by typing

cd <esd_filename_directory>

where

esd_filename_directory
is the directory with the iso image files, for example, SPFS009F.9F.R.NCL.NAP.VAULT.1.D

8 List the contents of the directory by typing

ls

Example response

```
platform_disk_1.iso.tape
platform_disk_2.iso.tape
platform_disk_3.iso.tape
```

9 Rename each file without the .tape extension by typing

mv <filename.tape> <filename>

and pressing the Enter key.

where

filename.tape
is the name of the file with the .tape extension

filename
is the name of the file without the .tape extension

Example

```
mv platform_disk_1.iso.tape platform_disk_1.iso
```

10 Log out of the ESD load repository server.

11 Perform the steps under Transferring an ISO image to an SPFS-based server on page 17 to continue with this procedure.

Transferring an ISO image to an SPFS-based server

ATTENTION
In a two-server configuration, you will transfer the ISO image to the active server.

At your workstation

1 Establish a connection to the SPFS-based server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server on page 27.

2 Make sure the server has the correct directories. Use the following table as reference to identify the directory required for the SPFS-based server type (component) to which the ISO image is to be transferred.

Component	Directory path
ERS 8600	/swd
GWC	/gwc
All other components	/data/esd_iso

List the directory for your component by typing

`# ls <directory>`

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

3 Use the following table to determine your next step.

If the response	Do
indicates no such directory exists	step 4
displays the name of the directory	step 5

4 Create the directory by typing

```
# mkdir <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

5 Display the available disk space in the directory by typing

```
# df -k <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data

Example response

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

6 Record the amount of available disk space, which is provided in kilobytes. You will need the information later in this procedure.

7 Change directory by typing

```
# cd <directory>
```

and pressing the Enter key.

where

directory
is /swd, /gwc, or /data/esd_iso

8 Start an FTP session with the ESD repository server by typing

```
# ftp <ESD_repository_server_ip>
```

and pressing the Enter key.

where

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

9 When prompted, enter your user ID and password.

10 List the directories on the ESD repository server by typing

```
ftp> ls
```

and pressing the Enter key.

11 Change directory to the drop box directory by typing

```
ftp> cd <dropbox_directory>
```

and pressing the Enter key.

where

dropbox_directory
is the name of the your dropbox directory.

12 List the contents of the drop box by typing

```
ftp> ls -l
```

and pressing the Enter key.

13 Change to the directory that contains the iso image files by typing

```
ftp> cd <esd_filename_directory>
```

where

esd_filename_directory
is the directory that contains the iso image files, for example, SPFS0091.91.R.NCL.NAP.VAULT.1.D

14 Locate the iso image file you want to transfer, and identify the size of the file, which is provided in bytes.

Note: Divide the number of bytes by 1024 to convert the size to kilobytes.

15 Compare the size of the iso image file with the amount of available space you recorded in step 6.

16 Use the following table to determine your next step.

If	Do
the server has enough available disk space	step 18
otherwise	step 17

17 Clear additional disk space following local office policy, before you continue with this procedure. If necessary, contact your next level of support.

18 Change the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

19 Transfer the iso image file to the SPFS-based server by typing

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

and pressing the Enter key.

where

iso_image
is the full name of the iso image file

Note: Do not transfer any file with a .tar.gz extension.

20 End the FTP session by typing

```
ftp> bye
```

and pressing the Enter key.

21 List the contents of the directory to ensure the files successfully transferred to the server by typing

```
# ls -l
```

and pressing the Enter key.

You are now ready to mount the iso image on the server.

22 Perform the steps under Mounting an ISO image on an SPFS-based server on page 20 to complete this procedure.

Mounting an ISO image on an SPFS-based server

ATTENTION
In a two-server configuration, you will mount the ISO image on the inactive server with the exception of the APS and Media Server 2000 ISO images, which you will mount on the active server.

At your workstation

1 Use the following table to determine your first step.

If	Do
you have a two-server configuration	step 2
otherwise	step 4

2 Use the following table to determine your next step.

If	Do
you are mounting the APS or Media Server 2000 iso image	step 4
otherwise	step 3

3 Establish a connection to the inactive server through telnet or SSH using the physical IP address of the inactive server, log in using the root user ID and password, and ensure you are on the inactive server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server on page 27.

4 Start the command line interface by typing

```
# cli
```

and pressing the Enter key.

5 Enter the number next to the Other option in the menu.

6 Enter the number next to the mount_image option in the menu.

7 Use the following table to determine your next step.

If the system response is	Do
`Enter full path to ISO image`	step 9
`ISO image Already Mounted`	step 8

8 Enter the number next to the umount_image option in the menu and retry step 6.

Note: If either command is unsuccessful a second time, contact your next level of support.

9 When prompted, enter the full path name of the iso image on the server by typing

<directory_path>/<iso_image>

and pressing the Enter key.

where

directory_path
is /swd, /gwc, or /data/esd_iso

iso_image
is the full name of the ISO image file

Note 1: Do not attempt to change directories to the /tmpmnt directory until the mount command is complete.

Note 2: Record the path of the ISO image file for ISO image file removal.

10 Use the following table to determine your next step.

If the response	Do
is a warning to unmount the image before removing the image file	step 11
indicates the path you provided does not exist	Verify the location and name of the image and retry step 8.
indicates an error creating the image device location	Retry step 8. An operating system error with the loopback file driver occurred. If the command fails a second time, contact your next level of support.
indicates an error mounting the file	Repeat the steps under Transferring an ISO image to an SPFS-based server on page 17. The ISO image is corrupt or the /tmpmnt directory has been deleted. If the procedure fails a second time, contact your next level of support.

11 Exit each menu level of the command line interface by typing

`select - x`

and pressing the Enter key.

12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Unmounting and removing an ISO image from an SPFS-based server

Application

Use this procedure to perform the following tasks:

- unmount an ISO image on the SPFS-based server
- remove an ISO image from the SPFS-based server

Prerequisites

Determine the node, active or inactive, on which this procedure needs to be performed.

Action

Unmounting an ISO image on an SPFS-based server

ATTENTION
In a two-server configuration, you will unmount the ISO image on the inactive server where you upgraded the software. This excludes the APS and Media Server 2000 ISO images, which you will unmount on the active server where you upgraded the software.

At your workstation

1 Change out of the /tmpmnt directory to prevent a umount failure by typing

```
# cd /
```

and pressing the Enter key.

2 Access the command line interface to unmount the ISO image by typing

```
# cli
```

and pressing the Enter key.

3 Enter the number next to the option `Other` in the menu.

4 Enter the number next to the option `umount_image` in the menu.

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

`select - x`

and pressing the Enter key.

You are now ready to remove the ISO image from the server.

6 Perform the steps under Removing an ISO image from an SPFS-based server on page 25 to complete this procedure.

Removing an ISO image from an SPFS-based server

ATTENTION
In a two-server configuration, you will remove the ISO image from the active server.

At your workstation

1 Use the following table to determine your first step.

If	Do
you have a two-server configuration	step 2
otherwise	step 4

2 Use the following table to determine your next step.

If	Do
you are removing the APS or Media Server 2000 iso image from the server	step 4
otherwise	step 3

3 Establish a connection to the active server through telnet or SSH using the physical IP address of the active server, log in using the root user ID and password, and ensure you are on the active server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server on page 27.

4 Navigate to the directory where the ISO image is located by typing

```
# cd <directory_path>
```

and pressing the Enter key.

where

directory_path
is /swd, /gwc, or /data/esd_iso

5 Remove the ISO image from the server by typing

```
# rm <loadname>
```

and pressing the Enter key.

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Logging in to an SPFS-based server

Application

Use this procedure to log in to a Server Platform Foundation Software (SPFS)-based server. This procedures provides the steps to establish a login session using SSH, which is secure, or telnet, which is not secure.

Some tasks will require that you log in to the server through the console (port A) using the root user ID and password.

Prerequisites

This procedure requires the following information:

- the IP address or host name of the server

  Note: In a two-server configuration, you need the physical IP address of the active or inactive server.

- a valid user id and password
- the root password if you need to perform a task on the server that requires root user privileges

Action

Perform the steps under one of the following headings to complete this procedure.

- Logging in using SSH on page 28
- Logging in using Telnet on page 30
- Logging in through the console on page 32

Logging in using SSH

At your workstation

1 Establish an SSH session.

If you have access to a server which supports the ssh command (Linux, for example) then proceed with step a below. Otherwise, connect to the server using an SSH client and proceed to step 2.

a Establish an SSH session to the server by typing

```
> ssh -l <user_id> <server>
```

where

user_id
is root or your user id

server
is the IP address or host name of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

2 Use the following table to determine your next step.

If you receive	Do
a message indicating a host authentication issue and a request to continue the connection	step 3
a prompt for a password	step 4

3

ATTENTION
The prompt indicates SSH is verifying whether the server is a trusted host for the workstation. SSH performs the verification the first time SSH is run on a workstation.

Continue the connection by typing

```
y
```

and pressing the Enter key.

4 Enter the password for root or your user id.

5 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 9
two-server configuration	step 6

6 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

7 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 8
inactive server and the response is ClusterIndicatorACT	step 8
active server and the response is ClusterIndicatorACT	step 9
inactive server and the response is ClusterIndicatorSTBY	step 9

8 You are logged in to the wrong server. Return to step a to log in to the other server.

9 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Logging in using Telnet

At your workstation

1 Establish a telnet session to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or hostname of the SPFS-based server, or the physical IP address of the active or inactive server as required, in a two-server configuration

2 When prompted, enter your userid.

3 When prompted, enter your password.

4 Use the following table to determine your next step.

If	Do
you need to log in as root	step 5
otherwise	step 7

5 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

6 When prompted, enter the root password.

7 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 11
two-server configuration	step 8

8 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

9 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 10
inactive server and the response is ClusterIndicatorACT	step 10
active server and the response is ClusterIndicatorACT	step 11
inactive server and the response is ClusterIndicatorSTBY	step 11

10 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

11 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Logging in through the console

At the console connected to the server

1 Log in to the server through the console (port A) using the root user ID and password. In a two-server configuration, log in to the the active or inactive server as required.

2 Use the following table to determine your next step.

If your server is a	Do
one-server configuration	step 6
two-server configuration	step 3

3 Ensure you are on the correct server by typing

```
# ubmstat
```

and pressing the Enter key.

4 Use the following table to determine your next step.

If you need to be on the	Do
active server and the response is ClusterIndicatorSTBY	step 5
inactive server and the response is ClusterIndicatorACT	step 5
active server and the response is ClusterIndicatorACT	step 6
inactive server and the response is ClusterIndicatorSTBY	step 6

5 You are logged in to the wrong server. Log out of this server and return to step 1 to log in to the other server.

6 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

Copying GWC software from an SFPS-based server to the boot server

Purpose of this procedure

This procedure describes how to copy GWC software loads from an SPFS-based server, such as the CS 2000 Management Tools server to the boot server for the GWC. The boot server can be any of the following devices:

- CS 2000 Core Manager
- Core and Billing Manager (CBM)

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

You must have already performed procedure Transferring and mounting an ISO image on an SPFS-based server on page 13.

Action

At the CS 2000 Management Tools terminal

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

2 List the contents of the directory you created in procedure Transferring and mounting an ISO image on an SPFS-based server on page 13 by typing

```
$ ls <directory_name>
```

and pressing the Enter key.

where

directory_name
is the directory path specified in step 2 of Transferring and mounting an ISO image on an SPFS-based server on page 13.

3 Locate the .rpm file by accessing the following directories.

```
cd /tmpmnt/noarch
```

Note: Record the name of the .rpm file. You will use this filename later.

4 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: 2
```

5 Install the software by typing

> 2

and pressing the Enter key.

6 When prompted, enter the .rpm filname recorded in step 3 and press the Enter key.

7 When prompted for the location of the .rpm file, enter the directory specified in step 3 of this procedure and press the Enter key.

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

> Y

and pressing the Enter key.

9 When prompted, continue collecting by typing.

> yes

and pressing the Enter key.

10 When prompted for the password, enter the root password of the CS 2000 Core Manager or CBM and press the Enter key.

11 The system displays messages telling of its progress through the process of installing the rpm package. The final messages it displays are as follows:

```
Installation of Platform Load Complete.

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

12 Press the Enter key.

System response

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

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

    Please choose one of the following:
```

13 Exit the installation program by typing

`# X`

and pressing the Enter key.

14 Change to the root directory by typing

`# cd /`

and pressing the Enter key.

15 Unmount the ESD file by typing

`# mount_iso.ksh umount`

and pressing the Enter key.

16 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 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.

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.

System response:

The script checks whether the appropriate configuration data is present in the /swd/gwc directory.

20 If prompted, enter the hostname of the CS 2000 Management Tools server (where the SAM21 EM server process resides) and press the Enter key. Otherwise, continue with step 22.

21 If prompted, enter the IP address of the CS 2000 Management Tools server (where the SAM21 EM server process resides) 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 the CS 2000 Management Tools terminal

23 Log out of the CS 2000 Management Tools server.

24 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Upgrade the GWC using the GWC Upgrade Tool

Purpose of this procedure

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

When to use this procedure

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

Prerequisites

The following prerequisites and guidelines apply to this procedure.

CAUTION

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

All the necessary patches must be loaded into the Network Patch Manager (NPM) application.

CS 2000 SAM21 Manager must be installed on the same server as the GWC Upgrade Tool. For the GWC Upgrade Tool to be launched, CORBA, SESMService, NPM, and CS 2000 SAM21 Manager software packages must be running in this server.

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

The NPM automated processes must be disabled. Refer to step 33 of this procedure for more information.

If the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to auto-negotiate. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before

launching the GWC Upgrade Tool. Refer to procedure Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate on page 101.

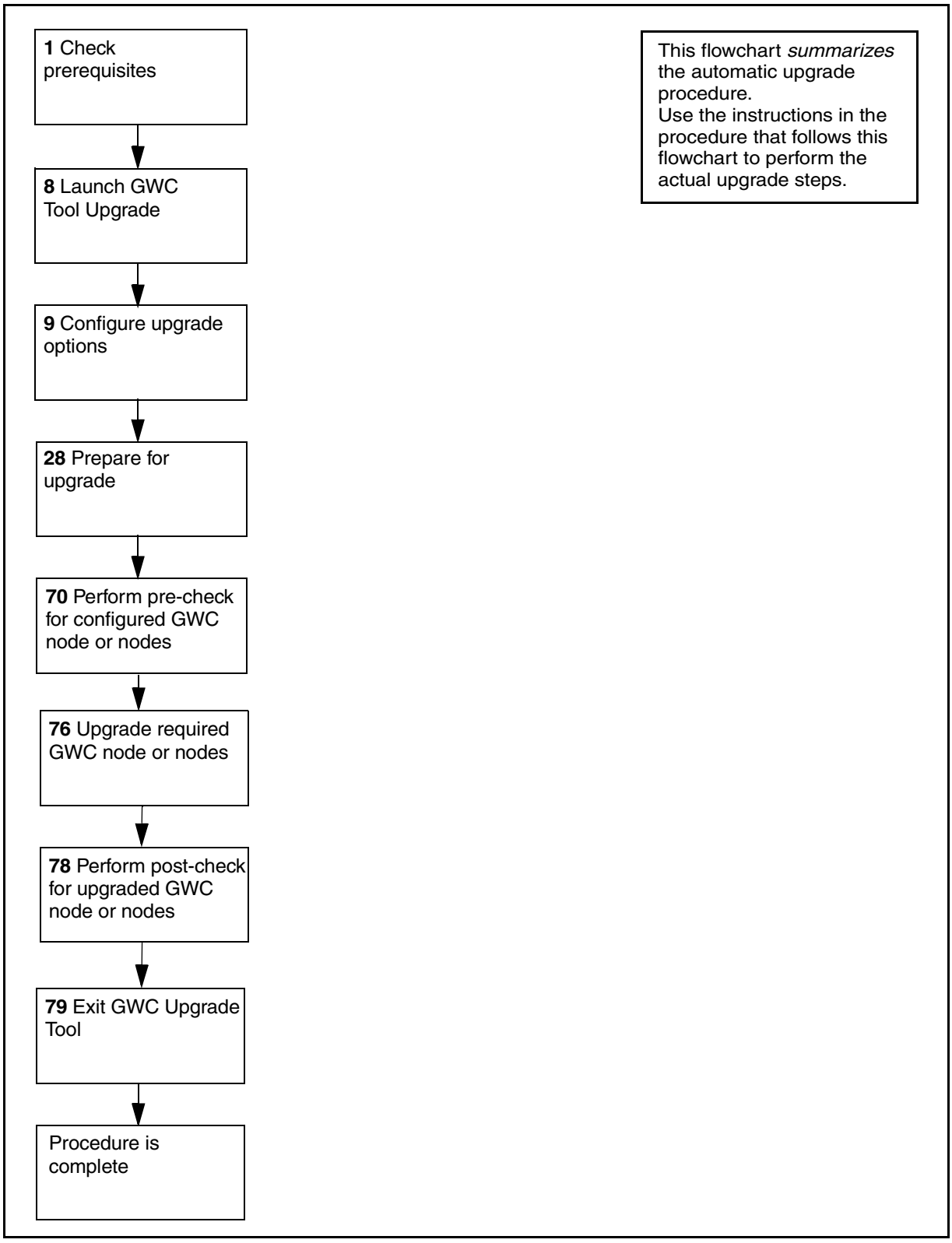
Overview

The GWC Upgrade Tool is distributed with the CS 2000 Management Tools SESM software package. The tool supports GWC upgrades using the command line user interface (CLUI). The tool automatically performs the following GWC upgrade operations:

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

The following flowchart provides an overview of the automated upgrade procedure. The numbers correlate to the steps of Action: upgrade procedure on page 44, following the flowchart.

Automatic upgrade overview



Configurable options

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

Option name	Mandatory (M) or optional (O)	Description	Default value
New Load File	M	The name of the new GWC load file.	
GWC List	M	The GWCs to be upgraded. By default, all GWC nodes managed by the CS 2000 GWC Manager and CS 2000 SAM21 Manager are selected.	All
Load Directory	O	The GWC load directory configured in CS 2000 SAM21 Manager. The default value is /swd/gwc. If the Core and Billing Manager (CBM) was used, the user must change the load directory to /gwc.	current configured load path
New Load Name	O	The target load name of the given GWC load file. If the file name does not contain the GWC load name, the user must specify a valid GWC load name here. The new load name is used to query the patch list from NPM. By default, the new load file name is LOAD_NAME.imag, for example, gn090ch.imag.	new load file name (excluding .imag')
Old Load Name	O	The load upgraded from. The default value is null. If the user ignores this option (the default), the upgrade manager server bypasses old load checking and all selected GWC nodes are upgraded automatically.	old load file name (excluding .imag')

Option name	Mandatory (M) or optional (O)	Description	Default value
Upgrade Mode	O	Defines whether GWCs are upgraded singly or together. Three modes are available: single - All GWC nodes are upgraded one by one, ordered by GWC profile type and GWC ID. bulk - All GWC nodes within the same service group (for example, TRUNK, LINE) are upgraded at the same time. If patching is needed, the first selected seed GWC node which is used to create the soak image uses single mode, and the other nodes that do not need patching use bulk mode. mix - In the same GWC profile group (for example, Trunk GWCs, Line GWCs), one GWC node is upgraded first. This enables the user to verify a specific type of GWC. After the first node is upgraded successfully, all the other GWC nodes within the same profile group are upgraded together.	bulk

Option name	Mandatory (M) or optional (O)	Description	Default value
Pause Point	O	Specifies the points at which the upgrade process pauses to allow the user to make manual checks. Seven options are available: 0 - No pause points; if 0 is selected, all other pause points are ignored. 1 - Pause before locking the first unit of the seed GWC node. 2 - Pause after patches are applied to the seed node. 3 - Pause before warm swact of the seed node. 4 - Pause after warm swact of the seed node. 5 - Pause after the seed node is upgraded. 6 - Pause before warm swact of non-seed nodes. Pause points 1 to 5 apply only to the seed GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.	0
Logging Level	O	Defines the default logging level of the GWC Upgrade Tool.	VRB
Max Time	O	Defines the time limit (in minutes) for the upgrade. If the upgrade cannot complete all the GWC nodes in the specified time, the non-upgraded GWCs remain un-upgraded and the process ends. The default value **0** disables the time limit check.	0 (no time limit)

Option name	Mandatory (M) or optional (O)	Description	Default value
Alarm Level	O	Defines the alarm level of the in-service GWC unit that the GWC Upgrade Tool reports to the user. Values are: MAJ - indicating a major alarm CRT - indicating a critical alarm	MAJ
Alarm Number	O	Defines the acceptable alarm count, that is, the number of in-service GWC alarms of the specified alarm level at which the GWC Upgrade Tool reports to the user (refer to section Alarm checking on page 43 in this procedure for details).	2

Alarm checking

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

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

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

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

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

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

Action: upgrade procedure

At the CS 2000 Management Tool interface

1 Check the prerequisites for this procedure as described in section Prerequisites on page 37.

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

3 Telnet or SSH to the CS 2000 Management Tools server. If your CS 2000 Management Tools resides in a high-availability cluster, make sure you log in to the active server.

Type:

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

and press the Enter key.

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

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

```
> id -a
```

and press the Enter key.

System response:

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

Group names

6 Change to the root user. Type

```
> su - root
```

and press the Enter key.

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

```
> servquery -status all
```

and press the Enter key.

System response:

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

Server states

8 Launch GWC Upgrade Tool

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

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

and press the Enter key.

System response:

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

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

x - Stop upgrade tool and exit CLUI

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

Note: If the GWC Upgrade Tool fails to start, check the logs. These are in the same directory as the tool, that is, gwcuptool/logs.

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

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

Example system response:

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

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

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

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

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

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

9 **Configure upgrade options**
From the Main Menu, enter:

> 2

System response:

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

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

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

10 Enter the name of the new GWC load file name. The load file name has a .imag extension. Make sure that the configured load file name exists on the CS 2000 Core Manager or CBM.

Load file name format:

nnnnnnn.nnnn

Example file name entry:

gn090bv.imag

System response:

```
Enter the new load file name(Example: gn070bv.imag): gn090bv.imag

[Step 2 - GWC LIST]
Separate GWC names with comma, for example: GWC-1,GWC-2,GWC-3,GWC-5

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

11 Enter the GWC nodes to be upgraded. To select all available GWCs, press the Enter key. To select specific GWCs, enter the names of those required (separated with commas and no spaces).

Note: If you select all available GWCs, the GWC Upgrade Tool automatically upgrades the card types in the correct order. Refer to section Upgrade order for GWC card types on page 5.

Example list entry:

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

The system displays the current input configuration values.

Example system response:

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

[Step 3 - INPUT VALUES]
New Load File Name    : gn090bv.imag
GWC List              : GWC-2,GWC-4
Default values
Load Directory        : /swd/gwc/
New Load Name         : "" (ignored)
Old Load Name         : "" (ignored)
Upgrade Mode          : bulk
Pause Point           : 0 (none)
Logging Level         : VRB
Max Time              : 0 (no limitation)
Alarm Level           : MAJ
Alarm Number          : 2

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

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

If	Do
you want to use the values	enter **Y** and go to step 28
you want to change the values	enter **N** and continue at step 13
your office uses a CBM	enter **N** and continue at step 13

Note: In the downgrade procedure, you must enter **N** to reject the default values, otherwise you cannot continue with step 13 and the rest of the downgrade steps.

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

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

[Step 4 - LOAD DIRECTORY]
Default load directory formats are different for SDM and CBM.
If SDM is used, it should be "/swd/gwc".
If CBM is used, it should be "/gwc".
Enter the load directory (Default: "/swd/gwc"):
```

14 Enter the load directory for CS 2000 Core Manager or CBM.

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

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

15 System response (after pressing Enter):

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

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

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

System response (after pressing Enter):

```
Enter the new load name (Default: ""): gn090bv

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

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

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

18 System response (after pressing Enter):

```
Enter the old load name (Default: ""): gn080bv

[Step 7 - UPGRADE MODE]
Values:
1 - single
2 - bulk
3 - mix
h - help
Enter the upgrade mode (1-3,h), (Default: 2):
```

19 Enter the upgrade mode (see section Configurable options on page 40.

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

20 System response (after pressing Enter):

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

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

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

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

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

21 Enter the pause points for the upgrade (see section Configurable options on page 40). Pause points allow you to carry out manual checks at selected intervals during the upgrade process. Pause points 1 to 5 (refer to the previous screen) apply only to the patched seed GWC node; pause point 6 applies to all other bulk upgrade GWC nodes.

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

Example pause point entry:

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

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

System response (after pressing Enter):

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

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

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

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

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

System response (after pressing Enter):

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

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

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

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

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

In the Prepare step (see step 28), this value is compared with the estimated time for the upgrade. If the upgrade cannot be completed within the given time limit, the Prepare step fails.

System response (after pressing Enter):

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

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

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

24 Enter the required alarm level: CRT or MAJ. For details, refer to section Alarm checking on page 43.

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

System response (after pressing Enter):

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

[Step 12 - ALARM NUMBER]

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

25 Enter the maximum number of alarms allowed during the upgrade. For details, refer to section Alarm checking on page 43. If the current alarm state has a higher priority than the alarm number defined in this entry, the upgrade process pauses and the system notifies the user.

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

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

System response (after pressing Enter):

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

Configuration values:
New Load File Name    : gn090bv.imag
GWC List              : GWC-2,GWC-4
Load Directory        : /swd/gwc
New Load Name         : gn090bv
Old Load Name         : gn080bm
Upgrade Mode          : bulk
Pause Point           : 0
Logging Level         : VRB
Max Time              : 0
Alarm Level           : MAJ
Alarm Number          : 2

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

26 Check the upgrade configuration options. Review the values displayed in the system response (shown in the previous screen) and decide whether or not to proceed with the upgrade.

If	Do
you want to confirm the upgrade configuration options	enter **Y**; note the following system response, and go to step 28
you do not want to confirm the upgrade configuration options	enter **N**, then go back to step 9 to re-enter the options, or go to step 80 to exit the GWC Upgrade Tool

27 System response:

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

Current configuration values:
 GWC load file: gn090bv.imag
 New load name: GN090BV
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: VRB

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

x - Stop upgrade tool and exit CLUI

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

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

Example system response:

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

Current configuration values:
 GWC load file: gn090bv.imag
 New load name: GN090BV
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: VRB

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

x - Stop upgrade tool and exit CLUI

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

28 **Prepare for upgrade**

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

> 4

System response:

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

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

x - exit

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

29 Select the Prepare option from the Upgrade Menu. Enter:

> 1

Example system response:

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

[1 Prepare step]

The following patches are available in NPM:
  1, NBF00G09
  2, NBF01G09
  3, NBF02G09
  4, NBF03G09
  5, NBF04G09
  6, NBF05G09
  7, NBF06G09
  8, NBF07G09
  9, NBF08G09
  10, NBF09G09
  11, NBF11G09
  12, NBF12G09
  13, NBF13G09
  14, NBF14G09
  15, NBF15G09
  16, NBF17G09
Please disable the NPM automated processes.
```

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

If	Do
upgrading using a CD-ROM	insert the upgrade CD-ROM into the 'active' CS 2000 Management Tools server, then go to step 32
upgrading using ESD	step 31

31 Check that the load is available in CS 2000 Core Manager or CBM. At the CS 2000 Management Tools server, type:

```
> cd /swd/gwc
> ls
```

and press the Enter key.

The system displays the loads in the GWC directory.

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

If the load	Do
is not available, the system displays the following message: `GWC load file doesn't exist. Please check and try later.` (see GWC load not available on page 71)	go back to step 10
is available	continue at step 33

33 Disable the NPM automated processes.

If you want to log in to the	Do
NPM GUI	continue at step 34
NPM CLUI	go to step 39

34 **NPM GUI**
Select System from the tool bar.

35 Select Plans from the menu.

36 Click on the Plan List tab.

37 If any of the plans in the list are Enabled, as indicated by the check mark, they must be disabled. For each plan that is

enabled, highlight the plan in the menu and click on the Disable button at the bottom.

38 Go to step 41.

39 **NPM CLUI**
Execute the command: vplan all

40 If any of the plans in the list have Enabled set to Y, they must be disabled.
For each plan that is enabled, execute the following command to disable it:
disableplan <planname> OFF

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

42 Display and confirm the patch list.

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

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

44 Telnet to the Sun server where the NPM resides.

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

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

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

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

If patches were delivered	Do
on CD-ROM	Continue at step 49
electronically	Go to step 54

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

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

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

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

53 Go to step 64.

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

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

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

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

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

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

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

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

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

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

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

Note: You can start NPM by typing **servstart NPM** and pressing the Enter key.

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

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

67 Retrieve the patch files for the NPM to process as follows:

If you want to retrieve the patches from	Do
CD-ROM	type **npm> getpatch** <current.patchlist> and press the Enter key
ESD	type **npm> getpatch** <patch_filename> and press the Enter key where <patch_filename> is the name of the file that contains names of the patch files to retrieve (the name must end with .patchlist), or an actual patch file

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

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

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

70 Eject the CD-ROM from the drive. Type **eject cdrom** and press the Enter key.

Example system response:

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

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

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

x - exit

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

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

71 **Perform pre-check**

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

> 2

Example system response:

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

[2 Pre-check step]

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

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

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

x - exit

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

72 Check the pre-check conditions. Review the information in the system response (refer to the previous screen) as described in step 73 to step 75.

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

74 Check that neither GWC card has a hardware alarm.

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

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

If	Do
any of the pre-check conditions is not met (see Pre-check failure on page 71)	resolve the error conditions (go to step 7 to activate the servers, clear any hardware alarms, correct the status of the GWC cards), then continue the upgrade process at step 77
all the pre-check conditions are met (screen displays `passed`)	continue the upgrade process at step 77

77 **Upgrade GWC nodes**
In the Upgrade Menu, select the Upgrade option. Enter:

```
> 3
```

Internal procedures
At the start of the upgrade, the GWC Upgrade Tool performs the pre-check again. During the upgrade, the system displays a continuous log of the upgrade status (the log freezing may indicate a problem with one of the internal upgrade procedures).

You can also use the query option (refer to section Query upgrade status on page 66) to display the upgrade status. If any unexpected problems occur, the system normally prompts you for a response or confirmation before continuing.

If pause points were enabled during configuration (see step 21), the tool pauses at the specified points and waits for you to carry out the required manual checks. When you have finished, enter Continue to continue the upgrade.

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

There are two different internal upgrade procedures:

- For the seed GWC node there are 16 steps. The seed node is based on the upgrade order of the GWC card types, and GWC node ID. The GWC Upgrade Tool automatically selects the seed node from the GWC list entered by the user (see step 11).
- For all other (non-seed) nodes there are 11 steps. The tool automatically upgrades the other nodes when the seed is upgraded successfully.

Example system response from the seed node:

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

[3 Upgrade step]

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

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

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

Upgrade steps for the seed GWC node

This section assumes that GWC-2 is the seed node, GWC-2 UNIT-0 is in service, GWC-2 UNIT-1 is hot-standby, the new load file name is gn090bv.imag, and the load version is GN090BV.

The GWC Upgrade Tool automatically performs the following actions in the order listed:

1. Busies the inactive unit GWC-2 UNIT-1 in the GWC EM.
2. Locks the inactive unit GWC-2 UNIT-1 in the SAM21 EM.
3. Provisions GWC-2 UNIT-1 with the new load gn090bv.imag in the SAM21 EM.
4. Unlocks GWC-2 UNIT-1 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-2 UNIT-1 to become hot-standby.
6. Busies the upgraded GWC-2 UNIT-1 in the GWC EM.
7. Carries out a device audit against GWC-2 UNIT-1 in NPM.
8. Applies all available patches to GWC-2 UNIT-1 in NPM.
9. Returns To Service the patched GWC-2 UNIT-1 in the GWC EM.
10. Waits for GWC-2 UNIT-1 to become hot-standby.
11. Saves the soaked GWC image to the CS 2000 Core Manager or CBM.

    Note: The gn090bv.imag is now a soaked load which contains all applicable patches for the GN090BV load.

12. Warm swacts the GWC-2 nodes: GWC-2 UNIT-1 provides service, and GWC-2 UNIT-0 is hot-standby.
13. Locks the inactive second unit GWC-2 UNIT-0 in the SAM21 EM.
14. Provisions GWC-2 UNIT-0 with the new soaked load gn090bv.imag in the SAM21 EM.
15. Unlocks GWC-2 UNIT-0 in the SAM21 EM.
16. Waits for the inactive/upgraded GWC-2 UNIT-0 to become hot-standby.

Example system response - non-seed nodes:

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

Upgrade steps for the non-seed GWC nodes

This section assumes that GWC-4 is a non-seed node, GWC-4 UNIT-1 is in service, GWC-4 UNIT-0 is hot-standby, the new load file name is gn090bv.imag, and it is a soaked load which contains all applicable patches for the GN090BV load.

The GWC Upgrade Tool automatically performs the following actions in the order listed:

1. Busies the inactive unit GWC-4 UNIT-0 in the GWC EM.
2. Locks the inactive unit GWC-4 UNIT-0 in the SAM21 EM.
3. Provisions GWC-4 UNIT-0 with the newly soaked load gn090bv.imag in the SAM21 EM.
4. Unlocks GWC-4 UNIT-0 in the SAM21 EM.
5. Waits for the inactive/upgraded GWC-4 UNIT-0 to become hot-standby.
6. Warm swacts the GWC-4 nodes: GWC-4 UNIT-0 provides service, and GWC-4 UNIT-1 is hot-standby.
7. Busies the hot-standby GWC-4 UNIT-1 in the GWC EM.
8. Locks the inactive second unit GWC-4 UNIT-1 in the SAM21 EM.
9. Provisions GWC-4 UNIT-1 with the new soaked load gn090bv.imag in the SAM21 EM.
10. Unlocks GWC-4 UNIT-1 in the SAM21 EM.
11. Waits for the inactive/upgraded GWC-4 UNIT-1 to become hot-standby.

Pause conditions

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

If	Do
the current upgrade state is a pause point that you configured (see step 21) (see Pause point on page 73)	carry out the required manual check, then enter Continue to continue the upgrade
NPM requires manual actions to be taken during the patching step (see Patch problem on page 74)	launch the NPM GUI or CLUI to perform the required actions, then return to the GWC Upgrade Tool and enter Continue to continue the upgrade
the GWC alarms (on the in-service unit) exceed the configured alarm level (see step 24 and step 25) (see Alarm level exceeded on page 74)	refer to section Alarm checking on page 43
an operation failed when the tool invoked the GWC EM, SAM21 EM or NPM functions (e.g. the GWC EM cannot save the GWC load image to CS 2000 Core Manager or CBM)	check and rectify the failed operation manually, then enter Retry to continue the upgrade
an operation timeout occurs (refer to the following screen), for example, the upgraded inactive unit is not hot-standby; refer to section Operation timeout on page 75	carry out the timed-out operation manually, then enter Retry to continue the upgrade

Note: **Query upgrade status**

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

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

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

System response:

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

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

x - exit

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

79 Perform post-check

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

> 5

Example system response:

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

[5 Post-check step]
--{ Group-1 }-------------------------------------------------------------------
  GWC-2 SMALL_LINENA ... passed
              GWC Node: GWC-2
               Profile: SMALL_LINENA
                Status:  Upgrade finished successfully.
            Start time: Mon Dec 13 05:36:12 EST 2004
             Stop time: Mon Dec 13 05:52:36 EST 2004
          Elapsed time: 16 minutes 23 seconds
    GWC-2-UNIT-1: 47.142.128.51
     States from GWCEM:
     Current load name: GN090BV
  Administrative state: unlocked(1)
     Operational state: enabled(1)
         Standby state: providingService(3)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-2-UNIT-0: 47.142.128.50
     States from GWCEM:
     Current load name: GN090BV
  Administrative state: unlocked(1)
     Operational state: enabled(1)
         Standby state: hotStandby(1)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

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

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

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

80 Exit GWC Upgrade Tool

When the post-check finishes, exit the Upgrade Menu and return to the Main Menu. Enter:

```
> x
```

System response:

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

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

x - Stop upgrade tool and exit CLUI

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

81 Use the following table to determine your next step.

If	Do
you want to upgrade further GWC nodes	go back to step 9
all the required GWCs have been upgraded	continue at step 82

82

CAUTION

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

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

After the upgrade completes, stop the GWC Upgrade Tool and exit the CLUI. Enter:

> x

Example system response:

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

83 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Example screens

GWC load not available

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

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

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

GWC upgrade configuration

[Step 1 - LOAD FILE NAME]
Enter the new load file name (Example: gn070bv.imag): gn090bv.imag
.
.
.
Upgrade Menu for GWC upgrade tool
1 - Prepare
2 - Pre-check
3 - Upgrade
4 - Query upgrade status
5 - Post-check

x - exit

Enter selection (1-5,x): 1

GWC load file doesn't exist.
Available GWC loads in the given directory in SDM/CBM:
  - GwcConfig.sh
  - gn080bf.imag
  - gn080bf_jg.imag
  - gn080bg1.imag
```

Pre-check failure

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

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

x - exit

Enter selection (1-5,x): 2

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

Pause point

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

```
[Step 8 - PAUSE POINTS]
Values:
0 - no pause points.
(1) For the first GWC node within the same GWC group.
1 - before lock first upgrade unit of "seed" node.
2 - after patch applied to "seed" unit.
3 - before warm-swact.
4 - after warm-swact.
5 - after "seed" node upgraded.

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

Separate numbers with comma, for example: 1,3,4
Enter the pause points (Default: 0):1,2,3,4,5

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

Message received from the server:

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

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

Message received from the server:

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

Patch problem

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

```
Group-1 started
GWC-2: Upgrade task started.
GWC-2 [1/16]  Busy the hot-standby first unit. (GWC-2-UNIT-1)
GWC-2 [2/16]  Lock the inactive first unit. (GWC-2-UNIT-1)
GWC-2 [3/16]  Change the load of the locked first unit. (GWC-2-UNIT-1)
GWC-2 [4/16]  Unlock the first unit. (GWC-2-UNIT-1)
GWC-2 [5/16]  Wait for the first unit to become hot-standby. (GWC-2-UNIT-1)
GWC-2 [6/16]  Upgraded first unit is hot-standby. (GWC-2-UNIT-1)
GWC-2 [7/16]  Apply patch to the upgraded first unit. (GWC-2-UNIT-1)
Patch NBF01G09 requires special attention:
  Ftp Error command
Patch NBF02G09 requires special attention:
  ERROR: Patch NBF01G09 needs to be applied in GWC-2-UNIT-1 before NBF02G09 can be
applied.
Patch NBF03G09 requires special attention:
  ERROR: Patch NBF01G09 needs to be applied in GWC-2-UNIT-1 before NBF03G09 can be
applied.
.
.
.

Message received from the server:

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

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

Alarm level exceeded

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

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

Message received from the server:

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

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

Operation timeout

If an operation timeout occurs, the upgrade does not necessarily fail. You can use the CS 2000 Management Tools client and SAM21 Manager client to check the status of the GWC card. After performing the timed-out operation manually (for example, locking the GWC card), you can enter Retry to allow the upgrade process to continue. Refer to the following figure for assistance.

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

Message received from the server:

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

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

Downgrade the GWC using the GWC Upgrade Tool

Purpose of this procedure

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

Apart from the GWC load image file names, use of the tool is the same as for upgrading (see Upgrade the GWC using the GWC Upgrade Tool on page 37). For an overview of the tool, refer to section Overview on page 38. For details of the configurable options, refer to section Configurable options on page 40.

When to use this procedure

Use this procedure if you want to return the GWC to the old load after upgrading the GWC using the GWC Upgrade Tool.

Prerequisites

The following prerequisites and guidelines apply to this procedure.

CAUTION

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

The upgraded GWC must not have any new data provisioned.

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

- Copying GWC software from CD to the boot server on page 110.
- Transferring and mounting an ISO image on an SPFS-based server on page 13.

All the necessary patches must be loaded into the Network Patch Manager (NPM) application.

CS 2000 SAM21 Manager must be installed on the same server as the GWC Upgrade Tool. For the GWC Upgrade Tool to be launched, CORBA, SESMService, NPM, and CS 2000 SAM21 Manager software packages must be running in this server.

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

The NPM automated processes must be disabled. Refer to step 33 of this procedure for more information.

If the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to auto-negotiate. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the GWC Upgrade Tool. Refer to procedure Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate on page 101

Action

At the CS 2000 Management Tools interface

1 Check the prerequisites for this procedure as described in section Prerequisites on page 77.

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

3 Telnet or SSH to the Sun server. Type:

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

and press the Enter key.

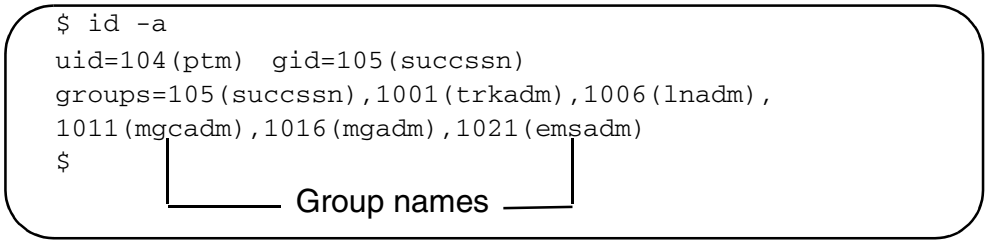
4 When prompted, type your user ID and password, and press the Enter key.

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

```
> id -a
```

and press the Enter key.

System response:



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

If you are	Do
logged in as root	go to step 7
not logged in as root	change to the root user; type **su - root** and continue at step 7

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

```
> servquery -status all
```

and press the Enter key.

System response:

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

Server states

8 Launch GWC Upgrade Tool

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

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

and press the Enter key.

System response:

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

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

x - Stop upgrade tool and exit CLUI

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

Note: If the GWC Upgrade Tool fails to start, check the logs. These are in the same directory as the tool, that is, gwcuptool/logs.

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

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

Example system response:

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

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

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

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

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

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

9 **Configure downgrade options**

From the Main Menu, enter:

> 2

System response:

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

x - Stop upgrade tool and exit CLUI

Enter selection (1-4,x): 2

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

10 Enter the GWC load file name. Ensure that the configured load file name exists on the CS 2000 Core Manager or CBM.

Load name format:

nnnnnnn.nnnn

Example file name entry:

gn090bv.imag

System response:

```
Enter the new load file name (Example: gn070bv.imag): gn080ch.imag

[Step 2 - GWC LIST]
Separate GWC names with comma, for example: GWC-1,GWC-2,GWC-3,GWC-5

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

11 Enter the GWC nodes to be downgraded. To select all available GWCs, press the Enter key. To select specific GWCs, enter the names of those required (separated with commas and no spaces).

Note: If you select all available GWCs, the GWC Upgrade Tool automatically downgrades the card types in the correct order.

Example list entry:

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

The system displays the current input configuration values.

Example system response:

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

[Step 3 - INPUT VALUES]
New Load File Name    : gn080ch.imag
GWC List              : GWC-2,GWC-4
Default values
Load Directory        : /swd/gwc/
New Load Name         : "" (ignored)
Old Load Name         : "" (ignored)
Upgrade Mode          : bulk
Pause Point           : 0 (none)
Logging Level         : MAJ
Max Time              : 0 (no limitation)
Alarm Level           : MAJ
Alarm Number          : 2

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

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

If you want to	Do
use the values	enter **Y** and go to step 28
change the values	enter **N** and continue at step 13

Note: In this downgrade procedure, you must enter **N** to reject the default values, otherwise you cannot continue with step 13 and the rest of the downgrade steps.

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

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

[Step 4 - LOAD DIRECTORY]
Default load directory formats are different for SDM and CBM.
If SDM is used, it should be "/swd/gwc".
If CBM is used, it should be "/gwc".

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

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

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

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

15 System response (after pressing Enter):

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

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

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

System response:

```
Enter the new load name (Default: ""): GN080CH

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

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

18 System response:

```
Enter the old load name (Default: ""): G1090BV

[Step 7 - UPGRADE MODE]
Values:
1 - single
2 - bulk
3 - mix
h - help
Enter the upgrade mode (1-3,h), (Default: 2):
```

19 Enter the upgrade mode (see section Configurable options on page 40.

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

20 System response (after pressing Enter):

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

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

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

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

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

21 Enter the pause points for the downgrade (see section Configurable options on page 40). Pause points allow you to carry out manual checks at selected intervals during the downgrade process. Pause points 1 to 5 (refer to the previous screen) apply only to the patched seed GWC node; pause point 6 applies to all other bulk downgrade GWC nodes.

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

Example pause point entry:

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

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

System response (after pressing Enter):

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

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

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

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

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

System response (after pressing Enter):

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

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

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

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

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

In the Prepare step (see step 28), this value is compared with the estimated time for the downgrade. If the downgrade cannot be completed within the given time limit, the Prepare step fails.

System response (after pressing Enter):

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

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

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

24 Enter the required alarm level: CRT or MAJ. For details, refer to section Alarm checking on page 43.

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

System response (after pressing Enter):

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

[Step 12 - ALARM NUMBER]

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

25 Enter the maximum number of alarms allowed during the downgrade. For details, refer to section Alarm checking on page 43. If the current alarm state has a higher priority than the alarm number defined in this entry, the downgrade process pauses and the system notifies the user.

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

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

System response (after pressing Enter):

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

Configuration values:
New Load File Name    : gn080ch.imag
GWC List              : GWC-2,GWC-4
Load Directory        : /swd/gwc
New Load Name         :
Old Load Name         :
Upgrade Mode          : bulk
Pause Point           : 0
Logging Level         : MAJ
Max Time              : 0
Alarm Level           : MAJ
Alarm Number          : 2

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

26 Check the downgrade configuration options. Review the values displayed in the system response (shown in the previous screen) and decide whether or not to proceed with the downgrade.

If	Do
you want to confirm the downgrade configuration options	enter **Y**; note the following system response, and go to step 28
you do not want to confirm the downgrade configuration options	enter **N**, then go back to step 9 to re-enter the options, or go to step 80 to exit the GWC Upgrade Tool

27 System response:

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

Current configuration values:
 GWC load file: gn080ch.imag
 New load name: GN080CH
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

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

x - Stop upgrade tool and exit CLUI

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

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

Example system response:

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

Current configuration values:
 GWC load file: gn080ch.imag
 New load name: GN080CH
Load directory: /swd/gwc
  Working mode: bulk
 Selcted nodes: GWC-2,GWC-4
  Pause points: 0
      Max time: unlimited
Ignored alarms: MAJ 2
 Logging level: MAJ

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

x - Stop upgrade tool and exit CLUI

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

28 **Prepare for downgrade**

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

> 4

System response:

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

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

x - exit

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

29 Select the Prepare option from the Upgrade Menu. Enter:

> 1

Example system response:

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

[1 Prepare step]

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

30 Insert the upgrade CD-ROM into the ‘active’ CS 2000 Management Tools server.

31 Check that the load is available in CS 2000 Core Manager or CBM. At the CS 2000 Management Tools server, type:

```
> cd /swd/gwc
> ls
```

and press the Enter key.

The system displays the loads in the GWC directory.

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

If the load	Do
is not available, the system displays the following message: `GWC load file doesn't exist. Please check and try later.` (see GWC load not available on page 71)	go back to step 10
is available	continue at step 33

33 Disable the NPM automated processes.

If you want to log in to the	Do
NPM GUI	continue at step 34
NPM CLUI	go to step 39

34 **NPM GUI**
Select System from the tool bar.

35 Select Plans from the menu.

36 Click on the Plan List tab.

37 If any of the plans in the list are Enabled, as indicated by the check mark, they must be disabled. For each plan that is enabled, highlight the plan in the menu and click on the Disable button at the bottom.

38 Go to step 41.

39 **NPM CLUI**
Execute the command: viewplan

40 If any of the plans in the list has Enabled set to Y, they must be disabled.

For each plan that is enabled, execute the following command to disable it:
disableplan <planname> OFF

41 **Record disabled plans**
Keep a record of the plans that were disabled. These plans must be re-enabled at the end of the downgrade process.

42 Display and confirm the patch list.

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

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

44 Telnet to the Sun server where the NPM resides.

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

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

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

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

If patches were delivered	Do
on CD-ROM	Continue at step 49
electronically	Go to step 54

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

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

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

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

53 Go to step 64.

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

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

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

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

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

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

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

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

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

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

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

Note: You can start NPM by typing **servstart NPM** and pressing the Enter key.

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

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

67 Retrieve the patch files for the NPM to process as follows:

If you want to retrieve the patches from	Do
CD-ROM	type **npm> getpatch** <current.patchlist> and press the Enter key

If you want to retrieve the patches from	Do
ESD	type **npm> getpatch** <patch_filename> and press the Enter key where <patch_filename> is the name of the file that contains names of the patch files to retrieve (the name must end with .patchlist), or an actual patch file

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

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

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

70 Eject the CD-ROM from the drive. Type **eject cdrom** and press the Enter key.

Example system response:

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

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

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

x - exit

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

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

71 **Perform pre-check**
In the Upgrade Menu, select the Pre-check option. Enter:

> 2

Example system response:

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

[2 Pre-check step]

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

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

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

x - exit

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

72 Check the pre-check conditions. Review the information in the system response (refer to the previous screen) as described in step 73 to step 75.

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

74 Check that neither GWC card has a hardware alarm.

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

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

If	Do
any of the pre-check conditions is not met (see Pre-check failure on page 71)	resolve the error conditions (go to step 6 to activate the servers, clear any hardware alarms, correct the status of the GWC cards), then continue the downgrade process at step 77
all the pre-check conditions are met (screen displays `passed`)	continue the downgrade process at step 77

77 **Downgrade GWC nodes**

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

```
> 3
```

Internal procedures

The GWC Upgrade Tool reboots the GWC cards using the old load. At the start of the downgrade, the GWC Upgrade Tool performs the pre-check again. During the downgrade, the system displays a continuous log of the downgrade status (the log freezing may indicate a problem with one of the internal downgrade procedures). If any unexpected problems occur, the system normally prompts you for a response or confirmation before continuing.

While the downgrade in progress, you can use the query option to display the downgrade status (option 4 - Query upgrade status in the Upgrade Menu; see page 95). To query the overall status of the downgrade, you can also launch another telnet or SSH session to the server and type the following command:

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

If pause points were enabled during configuration (see step 21), the tool pauses at the specified points and waits for you to carry out the required manual checks. When you have finished, enter Continue to continue the downgrade.

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

78 When the downgrade completes, the system reports the final service status of the downgraded GWC nodes and returns to the Upgrade Menu.

System response:

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

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

x - exit

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

79 Perform post-check

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

> 5

Example system response:

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

[5 Post-check step]
--{ Group-1 }-------------------------------------------------------------------
  GWC-2 SMALL_LINENA ... passed
              GWC Node: GWC-2
               Profile: SMALL_LINENA
                Status:  Upgrade finished successfully.
            Start time: Mon Dec 13 05:36:12 EST 2004
             Stop time: Mon Dec 13 05:52:36 EST 2004
          Elapsed time: 16 minutes 23 seconds
    GWC-2-UNIT-1: 47.142.128.51
     States from GWCEM:
     Current load name: GN080CH
  Administrative state: unlocked(1)
     Operational state: enabled(1)
         Standby state: providingService(3)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0
    GWC-2-UNIT-0: 47.142.128.50
     States from GWCEM:
     Current load name: GN080CH
  Administrative state: unlocked(1)
     Operational state: enabled(1)
         Standby state: hotStandby(1)
           Fault state: none(0)
           Alarm state: 00 00 00 00
            - Critical: 0
               - Major: 0
   States from SAM21EM:
           Card status: Unlocked
     Operational state: Enabled
    Availability state: None
          Total Alarms: 0
            - Critical: 0
               - Major: 0

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

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

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

80 **Exit GWC Upgrade Tool**
When the post-check finishes, press the Enter key to return to the Upgrade Menu.

System response:

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

x - exit

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

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

> x

System response:

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

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

x - Stop upgrade tool and exit CLUI

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

82 Use the following table to determine your next step.

If	Do
you want to downgrade further GWC nodes	go back to step 9
all the required GWCs have been downgraded	continue at step 83

83

CAUTION

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

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

After the downgrade completes, stop the GWC Upgrade Tool and exit the CLUI. Enter:

> x

Example system response:

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

84 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate

Purpose of this procedure

If the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch 8600 routers, the port on the CS LAN router must be set to auto-negotiate the Ethernet port speed and duplex state. The port is normally configured that way. However, if the setting is incorrect, the port must be reconfigured before launching the SAM21 Shelf Controller or Gateway Controller upgrade tool.

When to use this procedure

If the Ethernet port on the CS LAN router is not set to auto-negotiate, use this procedure before launching the Shelf Controller or Gateway Controller upgrade tool.

Prerequisites

You must use READ/WRITE/ALL (RWA) login and/or password privileges when performing this procedure. For more information about RWA privileges, refer to the Ethernet Routing Switch 8600 configuration documentation.

Action

At the CLI for the Ethernet Routing Switch 8600

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

```
> show ip arp info <ip_address>
```

and press the Enter key

where <ip_address>
is the physical IP address of the Shelf Controller, Gateway Controller, or Universal SignalingPoint.

Example system response:

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

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

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

2 Use the values recorded in step 1 to set the slot and port to auto-negotiate. Type:

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

and press the Enter key.

System response:

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

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

3 Verify the port configuration. Type:

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

and press the Enter key.

System response:

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

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

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

The system displays the slot and port configuration.

4 Commit the change. Type:

`> save config`

and press the Enter key.

5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

GWC provisioning on MCS

Purpose of this procedure

This procedure modifies the GWC tab in MCS 5200 Provisioning Manager to indicate the correct MCS discriminator file. This action is necessary to ensure successful MCS-CS 2000 interworking.

When to use this procedure

Use this procedure after completion of a GWC load upgrade in a CS 2000 environment.

Prerequisites

This procedure has no prerequisites.

Action

At the MCS 5200 Provisioning Manager

1 Select the Provisioning client.

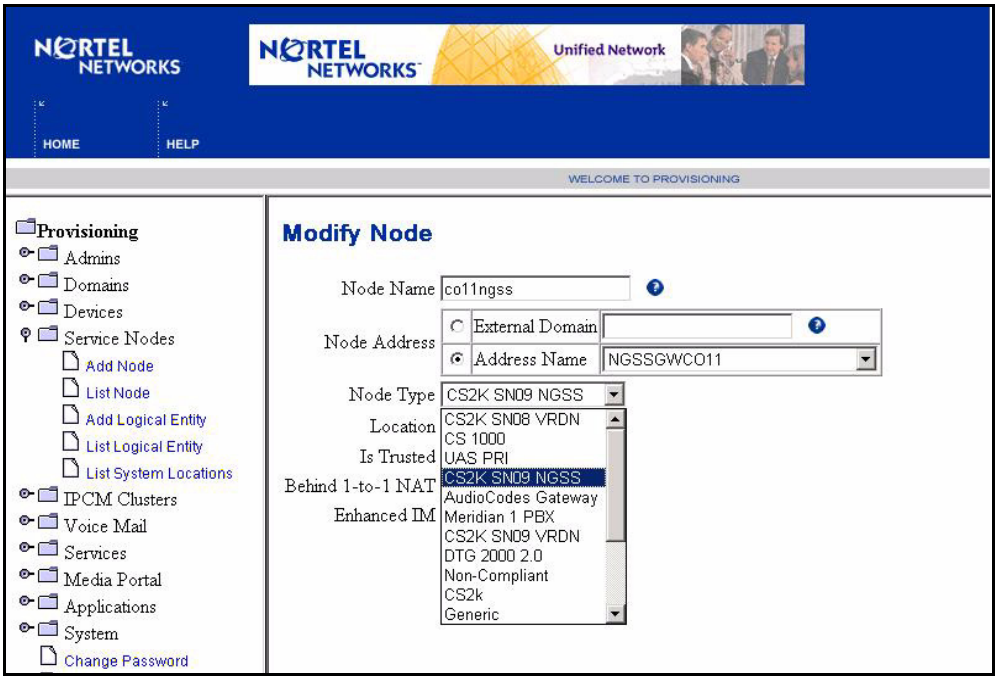
2 Select Service Nodes.

3 Select List Node.

4 Select the Node Name for the required GWC.

5 Select the Node Type drop-down menu.

Example system response:



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

If you just completed a	Do
Session Server GWC upgrade	select Node Type CS2K SN09 NGSS
VRDN GWC upgrade	select Node Type CS2K SN09 VRDN

7 Select Update.

8 Repeat step 4 to step 7 of this procedure for each MCS gateway whose gateway host points to this CS 2000.

9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Overall GWC upgrade process - manual

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

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

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

Prerequisites

The following prerequisites apply to this procedure:

ATTENTION

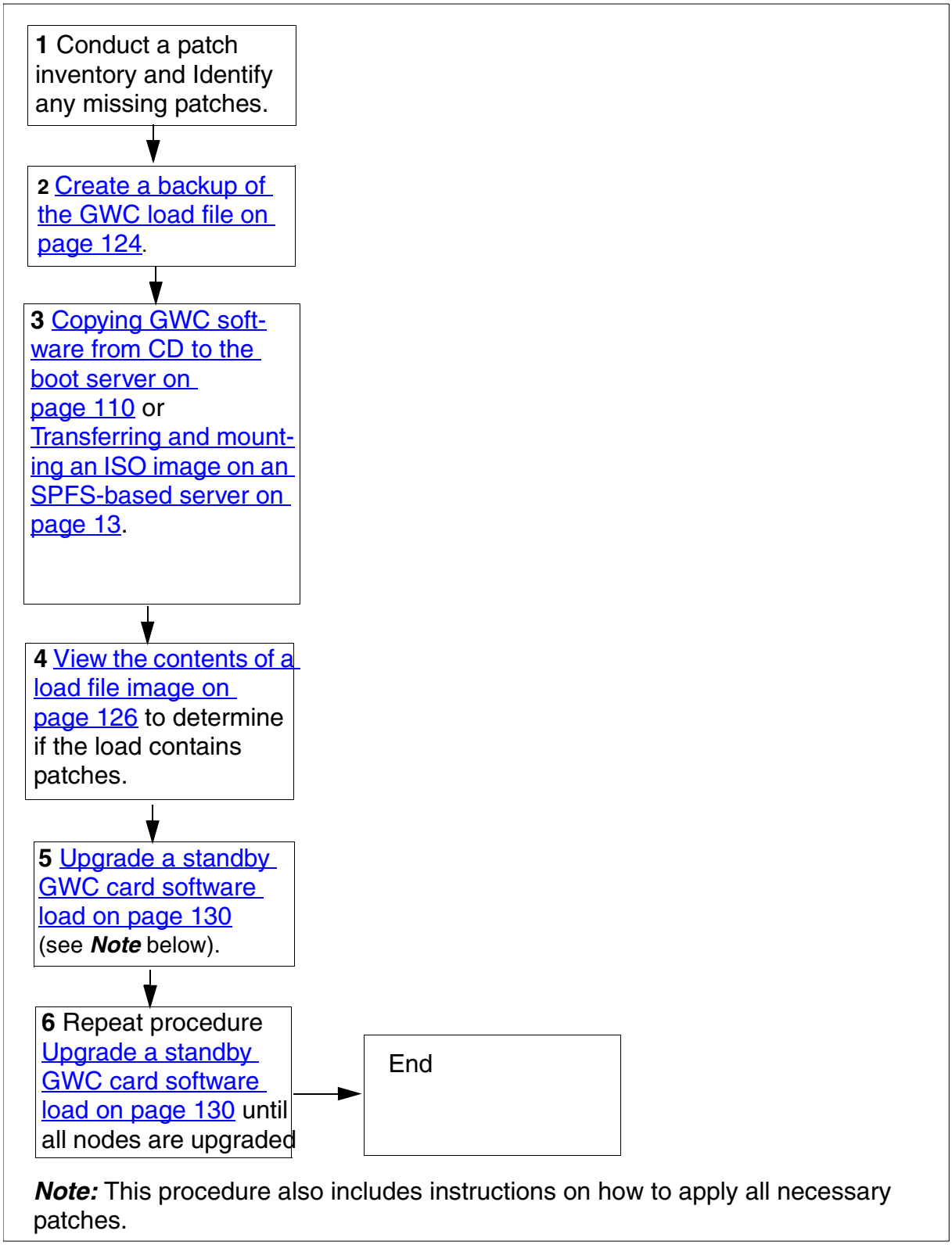
For IP network solutions only (starting in SN07), the call agent identifier (ID) must be set for the CS 2000. This must be done prior to upgrading your GWC cards. For details, refer to section "CS 2000 call agent identifier" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Before you begin, make sure that you have researched and addressed all the preparatory items described in procedure Preparing to upgrade the GWC on page 9.

Summary flowchart

The following flowchart summarizes the overall manual GWC upgrade process. The numbers relate to the steps of the detailed procedure in section Overall GWC upgrade procedure on page 108 following the flowchart.

Summary of the overall manual GWC upgrade procedure



Overall GWC upgrade procedure

1. If necessary, obtain one or more of the patch auditing tools available from www.nortelnetworks.com support site. To obtain the tools:
2. Under Support & Training, select Software Downloads.
3. Select the Browse Product Support tab (this is usually the default choice).
4. For Product Families, select Succession or Succession Communication Server 2000.
5. For Product menu, select Communication Server 2000.
6. For Content menu, select Tools, then click Go.
7. For instructions on how to install and use each tool, refer to the Readme file that can be found under each corresponding link.
8. 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 your site and retrieve the patch files for the NPM to process using the NPM CLUI getpatch command.
9. Perform a site-specific audit to identify any missing patches - use the Patch Audit or Inform List tool.
10. If necessary, backup your existing software load using procedure Create a backup of the GWC load file on page 124
11. If necessary, install the new load using one of the following methods:
    - Copying GWC software from CD to the boot server on page 110
    - Transferring and mounting an ISO image on an SPFS-based server on page 13
12. Determine if any patches are contained within the load image by completing procedure View the contents of a load file image on page 126
13. If a day or more has passed between completing step 8 and performing the upgrade, return to step 9 and continue.
14. Upgrade the software on a seed GWC unit that is inactive by completing procedure Upgrade a standby GWC card software load on page 130

15 Repeat step step 14 to upgrade each GWC node with the patched load until all units in each node are rebooted from the new image.

16 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Copying GWC software from CD to the boot server

Purpose of this procedure

This procedure describes how to copy GWC software from a CD to the boot server. The boot server for the GWC can be any of the following devices:

- CS 2000 Core Manager
- Core and Billing Manager (CBM)

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

1 Insert the CD-ROM into the CD-ROM tray of the 'active' CS 2000 Management Tools server.

At the CS 2000 Management Tools terminal

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

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

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

3 Execute the installation script by typing

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

and pressing the Enter key.

Example response:

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

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

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

  Please choose one of the following: 1
```

4 Install the software by typing

> 1

and pressing the Enter key.

The system displays the contents of the RPM package.

Example response:

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

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

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

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

`> Y`

and pressing the Enter key.

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

Example response:

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

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

6 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. 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*******
```

Note: An additional confirmation prompt can display requesting acceptance of the RSA key. Confirm the following sample prompt by typing yes.

```
RSA key fingerprint is 99:09:e2:80:57:95:3e:be:26:08:a0:c6:32:ed:48.
Are you sure you want to continue connecting (yes/no)?
```

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

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.

System response:

The script checks whether the appropriate configuration data is present in the /swd/gwc directory.

12 If prompted, enter the hostname of the CS 2000 Management Tools server (where the SAM21 EM server process resides) and press the Enter key. Otherwise, continue with step 14.

13 If prompted, enter the IP address of the CS 2000 Management Tools server (where the SAM21 EM server process resides) 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 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure

Transferring patches delivered on CD to the NPM database

Application

Use this procedure when you received a patch CD with the software release you are upgrading to, and you need to transfer the patches to the Network Patch Manager (NPM) database and retrieve them for processing.

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

Also use this procedure when you are either attempting to apply patches that have a blank patch category, or you are preparing for an HA cluster upgrade.

Prerequisites

You must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP solution-level Security and Administration*, NN10402-600.

Action

Perform the steps that follow to complete this procedure.

At the server

1 Insert the CD that contains the patches into the drive of the SPFS-based server where the NPM resides. In a two-server configuration, insert the CD into the drive of the active server.

At your workstation

2 Establish a connection to the server through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server on page 27.

3 Make a temporary directory for the patchlist file by typing

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

and pressing the Enter key.

4 Change the permissions on the temporary directory by typing

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

and pressing the Enter key.

5 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.

6 Access the directory you just created by typing

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

and pressing the Enter key.

7 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 8
running	step 9

8 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

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

```
# npm
```

and pressing the Enter key.

10 When prompted, enter your user ID and password.

Note: Do not change directories.

11 Retrieve the patch files copied from the CD by typing

```
npm> getpatch current.patchlist
```

and pressing the Enter key.

Note 1: Ignore the following error message which may appear if an older load cannot verify a patch for a newer load:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

Note 2: The golden directory mentioned in the previous note is /data/npm/Au. The files are successfully placed here when the getpatch is done, even though it appears to fail.

12 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

13 Change to the root directory level by typing

```
# cd /
```

and pressing the Enter key.

14 Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

If the DVD drive tray will not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands:

```
# /etc/init.d/volmgt stop
```

and pressing the Enter key.

```
# /etc/init.d/volmgt start
```

and pressing the Enter key.

Then, press the eject button located on the front of the DVD drive.

15 Remove the CD or DVD from the drive.

If	Do
you have other patch CDs to install	insert the next CD and go to step 5
otherwise	close the cdrom tray and proceed to the next step

16 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Transferring patches delivered through ESD to the NPM database

Application

Use this procedure when you received new patches after the software release through Electronic Software Delivery (ESD), and you need to transfer the patches to the Network Patch Manager (NPM) database and retrieve them for processing.

Prerequisites

This procedure has the following prerequisites:

- You must know the name or IP address of the load repository server and the location of the dropbox directory on the server.
- You must know the name or IP address of the SPFS-based server that is hosting the NPM.
- You must know the root password to the SPFS-based server.

Action

Perform the steps that follow complete this procedure.

Obtaining the NPM patch files from ESD

At your workstation

1 Establish a connection to the server that is hosting the NPM through telnet or SSH, and log in using the root user ID and password.

In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the **`ubmstat`** command.

For detailed steps, refer to procedure Logging in to an SPFS-based server on page 27.

2 Make a directory for the patch files you want to download by typing

```
# mkdir /<directory>
```

and pressing the Enter key.

where

directory
is a valid directory name

Example

```
# mkdir /esd_patches
```

3 Change the permissions on the newly created directory by typing

```
# chmod 777 /<directory>
```

and pressing the Enter key.

where

directory
is the directory name from step 2

Example

```
# chmod 777 /esd_patches
```

4 Access the newly created directory by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory
is the directory name from step 2

Example

```
# cd /esd_patches
```

5 Log in to the ESD server through FTP by typing

```
# ftp <esd_server>
```

and pressing the Enter key.

where

esd_server
is the IP address of the ESD server

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

7 Obtain a list of files and directories on the ESD server by typing

```
ftp> dir
```

and pressing the Enter key.

Note the name and timestamp of the .iso file.

8 Set the transfer mode to binary by typing

```
ftp> bin
```

and pressing the Enter key.

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

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

and pressing the Enter key.

To transfer individual patch files, type

```
ftp> get <patchfilename>
```

where

patchfilename
is the name of the patch you are transferring

10 Exit FTP by typing

```
ftp> quit
```

and pressing the Enter key.

11 Verify the patches are on the server in the temporary directory that you created in step 2 by typing

```
# ls
```

and pressing the Enter key.

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

```
# chmod 777 *
```

and pressing the Enter key.

13 Use the following table to determine your next step:

If	Do
you have access to http://www.nortel.com	step 14
you do not have access to http://www.nortel.com	step 15

14 Retrieve the patches that have been released since the software was shipped by using the Pre Upgrade Patch Calculator. The Pre Upgrade Patch Calculator will require a label and a date. The label is the first eight characters of the .iso file associated with the software component being upgraded and the date is the date of the file shown in step 7.

15 Create a patchlist file by typing

```
# ls *.patch > current.patchlist
```

and pressing the Enter key.

16 Verify the NPM server application is running by typing

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

and pressing the Enter key.

17 Use the following table to determine your next step:

If the NPM server is	Do
running	step 19
not running	step 18

18 Start the NPM server application by typing

```
# servstart NPM
```

and pressing the Enter key.

19 Ensure you are in the directory where you downloaded the patches by typing

```
# pwd
```

and pressing the Enter key.

The response must be the directory you created in step 2.

Example response

```
/esd_patches
```

If	Do
you are in the directory where you downloaded the patches	step 21
otherwise	step 20

20 Access the directory by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory
is the directory you created in step 2 to download the patches

Example

```
# cd /esd_patches
```

21 Access the NPM command line interface (CLUI) by typing

```
# npm
```

and pressing the Enter key.

22 When prompted, enter your user ID and password.

23 Retrieve the patch files for the NPM to process by typing

```
npm> getpatch current.patchlist
```

and pressing the Enter key.

Note 1: The following error message may be received when executing this step:

```
Error: Patch file
/data/npm/patch_upgrade/lex83o9s.ptchoamp
cannot be verified. Copying to golden
directory.
```

This is acceptable behavior because the current load cannot verify the patch from a higher load. Ignore this error.

Note 2: The golden directory mentioned in the previous note is /data/npm/Au. The files are successfully placed here when the getpatch is done, even though it appears to fail.

24 Exit the NPM CLUI by typing

```
npm> quit
```

and pressing the Enter key.

25 Access the directory that contains the downloaded patch files by typing

```
# cd /<directory>
```

and pressing the Enter key.

where

directory
is the directory you created in step 2 for the patch files

Example

```
# cd /esd_patches
```

26 Erase the downloaded patch files from the directory by typing

```
# rm *.patch
```

and pressing the Enter key.

27 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Create a backup of the GWC load file

Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a backup 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.

CAUTION
Possible rollback failure
If a backup is not created, the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM, preventing a rollback.

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.

There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of

a specific GWC card or node, refer to procedure “View the operational status of a GWC” in *Gateway Controller Configuration Management*, NN10205-511, to locate the load filename associated with a specific GWC card.

5

CAUTION

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

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

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

and pressing the Enter key.

where

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

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 You have completed this procedure. Return to Upgrading the GWC on page 10.

View the contents of a load file image

Purpose of this procedure

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

Perform this procedure on the CS 2000 Management Tools server since the gwclfinfo command is a SESM application script, and the /swd/gwc load directory is NFS-mounted on the CS 2000 Management Tools server in the /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 the delivered load contains patches.

Prerequisites

This procedure has no prerequisites.

Action

Use the following table to determine your first step.

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

At the CS 2000 Management Tools server

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

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

and pressing the Enter key.

2 List all the GWC load names by typing

```
# ls
```

and pressing the Enter key.

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

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

and pressing the Enter key.

where

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

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

Example response:

```
Load information from pgc09bl_patched_03_04.imag

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

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

4 Go to step 14

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 You have completed this procedure. Return to Upgrading the GWC on page 10.

Upgrade a standby GWC card software load

Purpose of this procedure

This procedure describes how to upgrade the software on a standby GWC card.

When to use this procedure

Use this procedure after installing a new version of the GWC software load on to the boot server where GWC software loads reside. The boot server is one of the following devices:

- CS 2000 Core Manager
- Core and Billing Manager (CBM)

Perform this procedure on each GWC node to be upgraded.

Prerequisites and guidelines

CAUTION

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

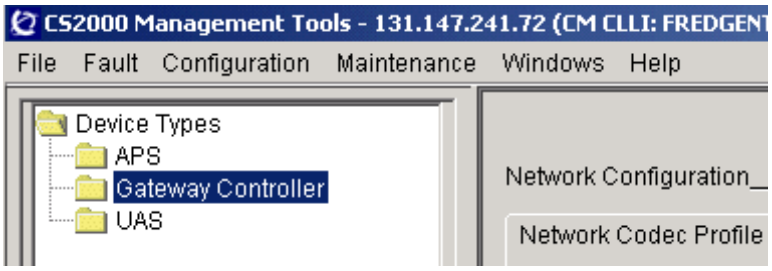
Perform the procedure Preparing to upgrade the GWC on page 9 before you begin this procedure.

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 7 in this procedure.

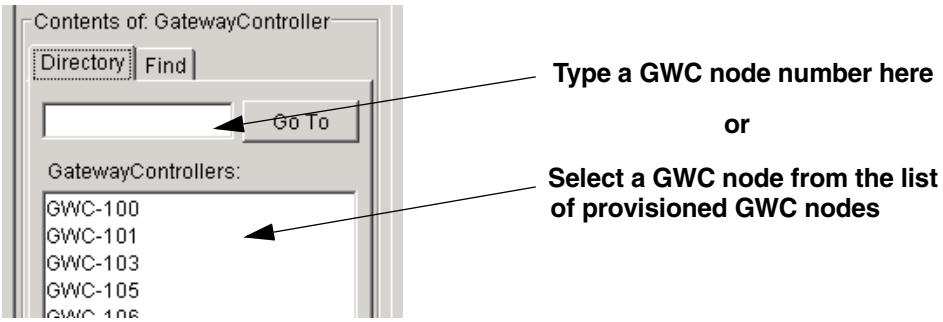
Action

At the CS 2000 GWC Manager client

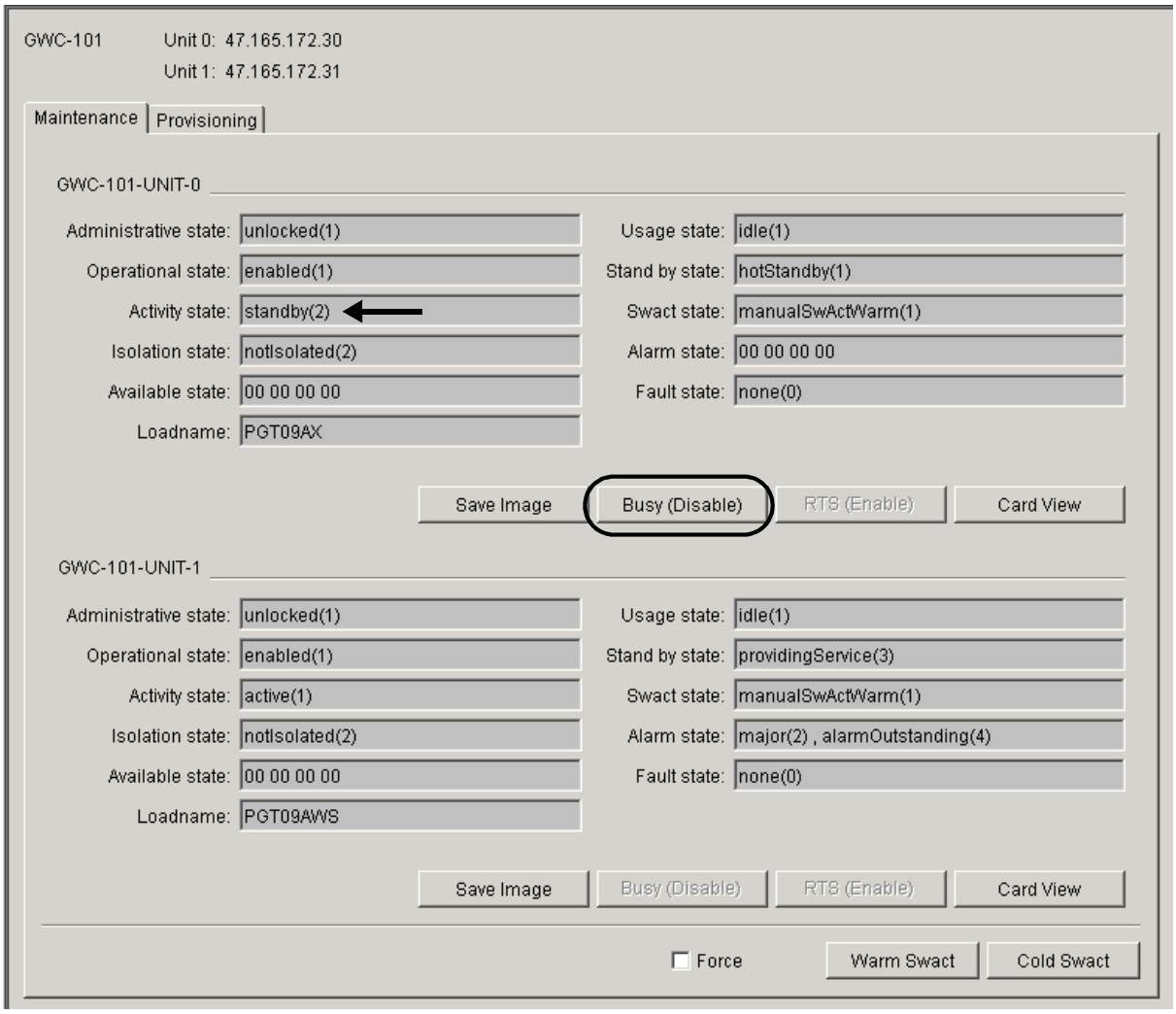
1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



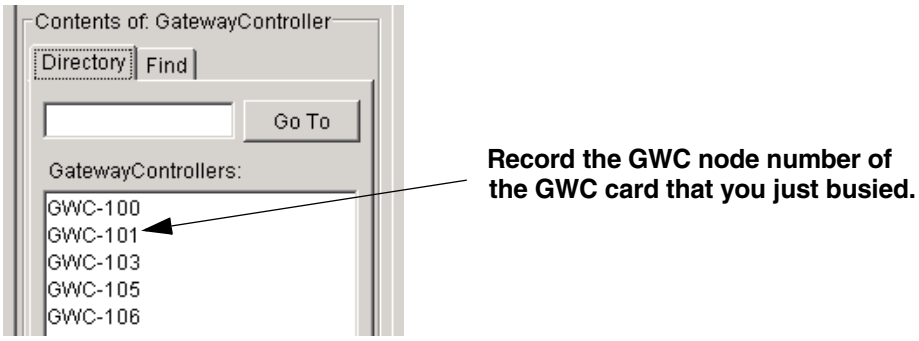
2 From the Contents of: Gateway Controller frame, select the GWC node that you wish to busy for an upgrade.



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

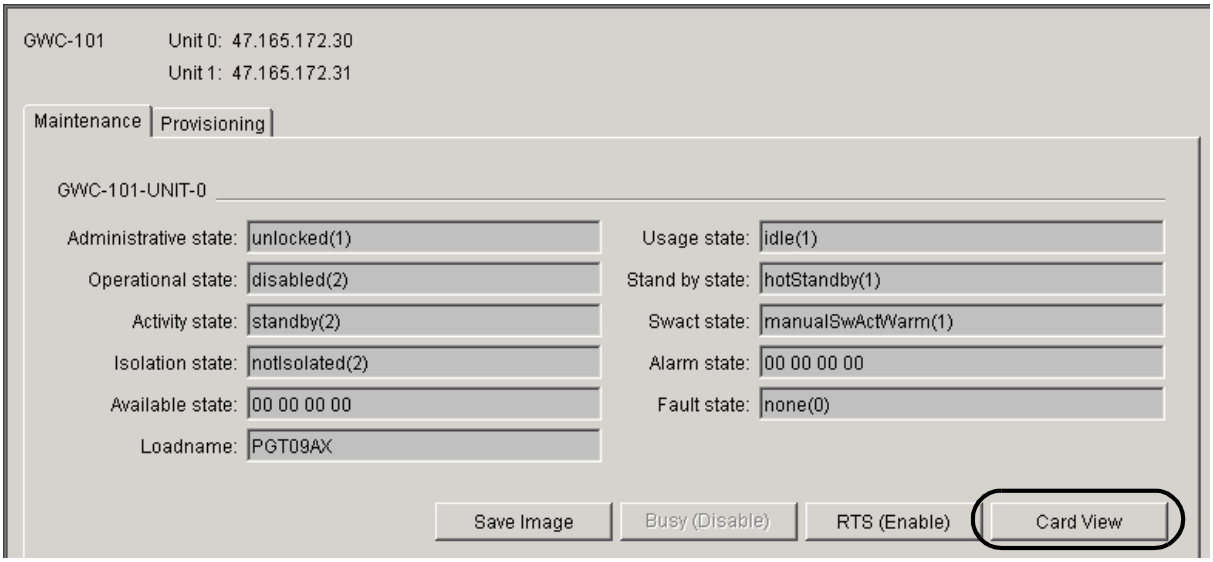


4 From the Contents of: Gateway Controller record the GWC node number for the GWC card you just busied. You will need this information later in this procedure.



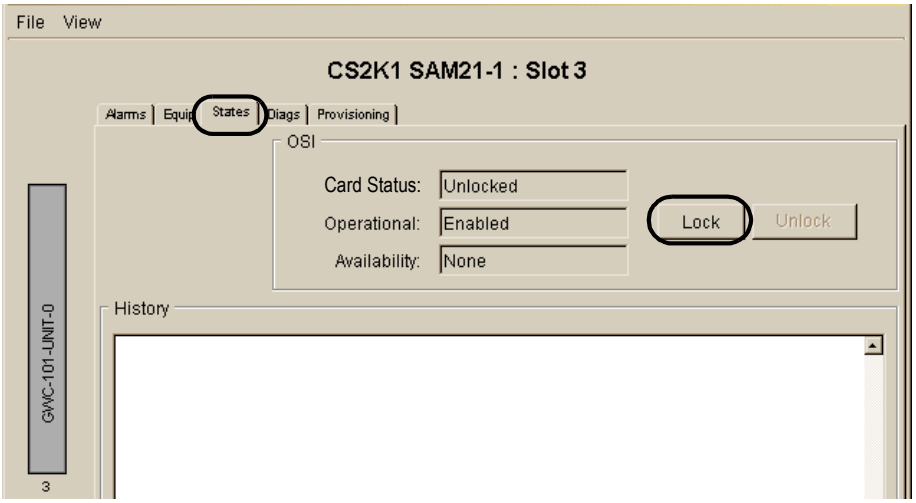
At the CS 2000 GWC Manager client

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

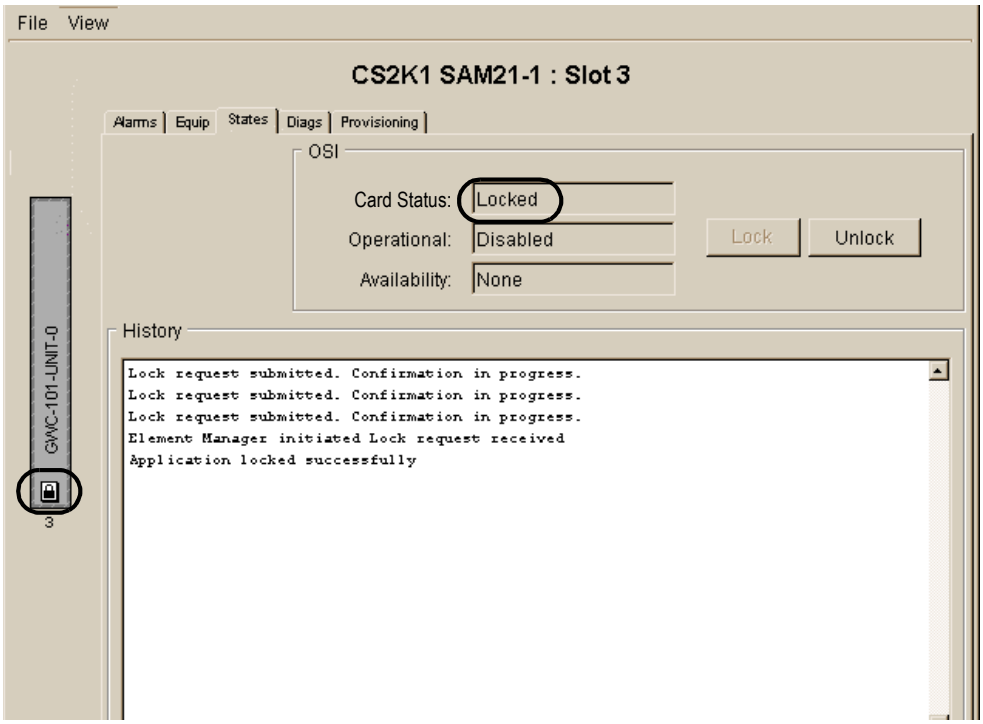


At the CS 2000 SAM21 Manager client

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


File View
CS2K1 SAM21-1 : Slot 3
Alarms
Equip
States
Diags
Provisioning
OSI
Card Status:
Unlocked
Operational:
Enabled
Availability:
None
Lock
Unlock
History
GWC-101-UNIT-0
3

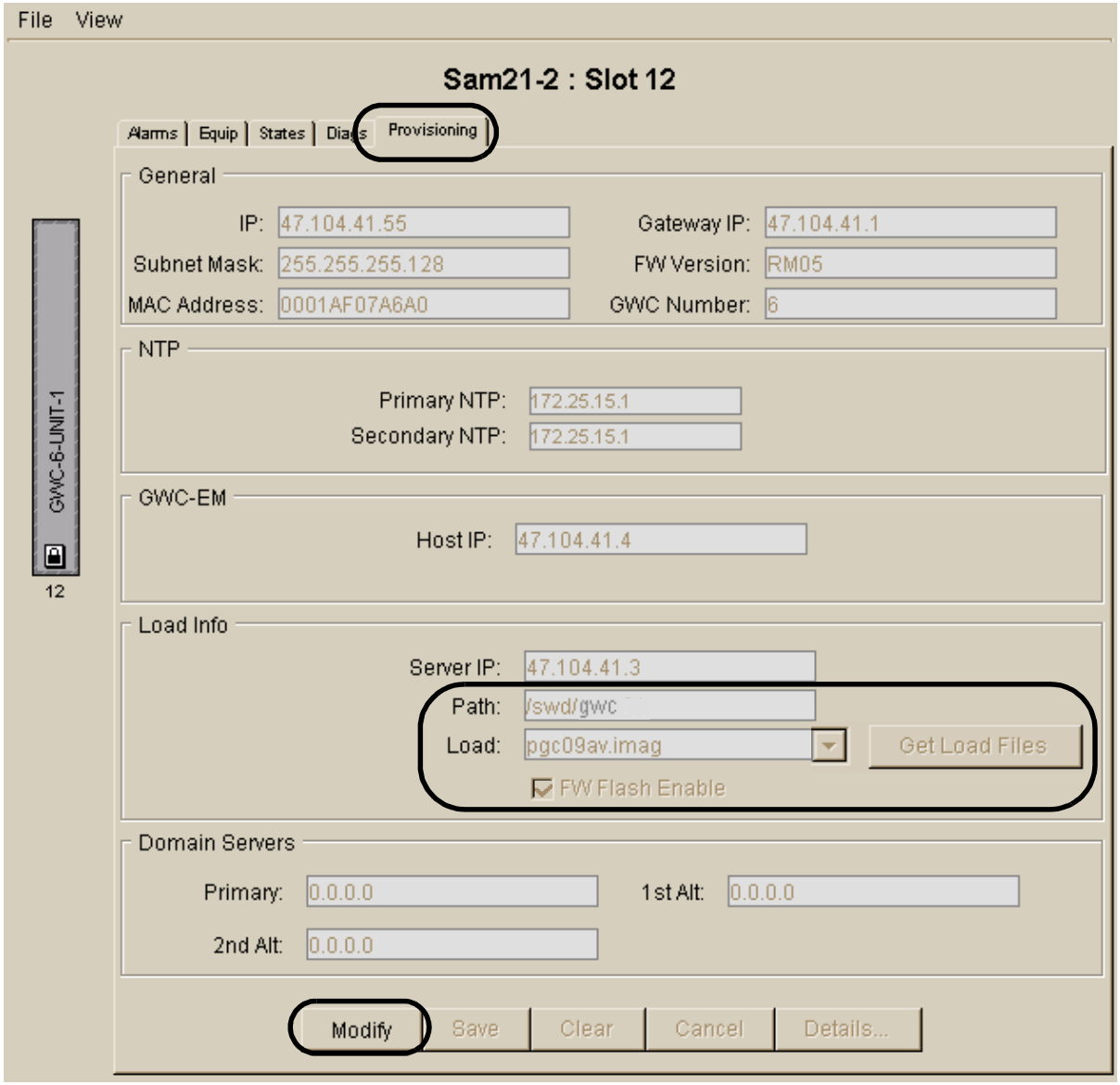
7 Observe the History display to confirm that the card has been locked. Look for the message: Application locked successfully. Also, notice the lock icon on the card graphic at the left of the screen and the Card Status indicating a Locked state.



8 Use the following table to determine your next step.

If	Do
the Communication Server LAN (CS LAN) is provided by Nortel Ethernet Routing Switch (ERS) 8000 series	Reprovision the port on the routing switch to auto-negotiate according to procedure Reprovision the Ethernet Routing Switch 8600 port to auto-negotiate on page 101. When reprovisioning is complete, continue at step 9.
the Communication Server LAN (CS LAN) is provided by a switch other than Nortel Ethernet Routing Switch (ERS) 8000 series	Reprovision the port on the routing switch to auto-negotiate according to the appropriate router product documentation. When reprovisioning is complete, continue at step 9.

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



10

CAUTION

For CS 2000 Core Manager the Path: field must be set to /swd/gwc; For CBM the Path: field must be set to /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.

Click the Get Load Files button (shown in the previous figure) and select the required load from the drop-down list.

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

11 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 12
otherwise	go to step 13

12 Type the GWC number in the GWC Number: field that you recorded in step 4 of this procedure. Refer to the following figure to locate these fields.

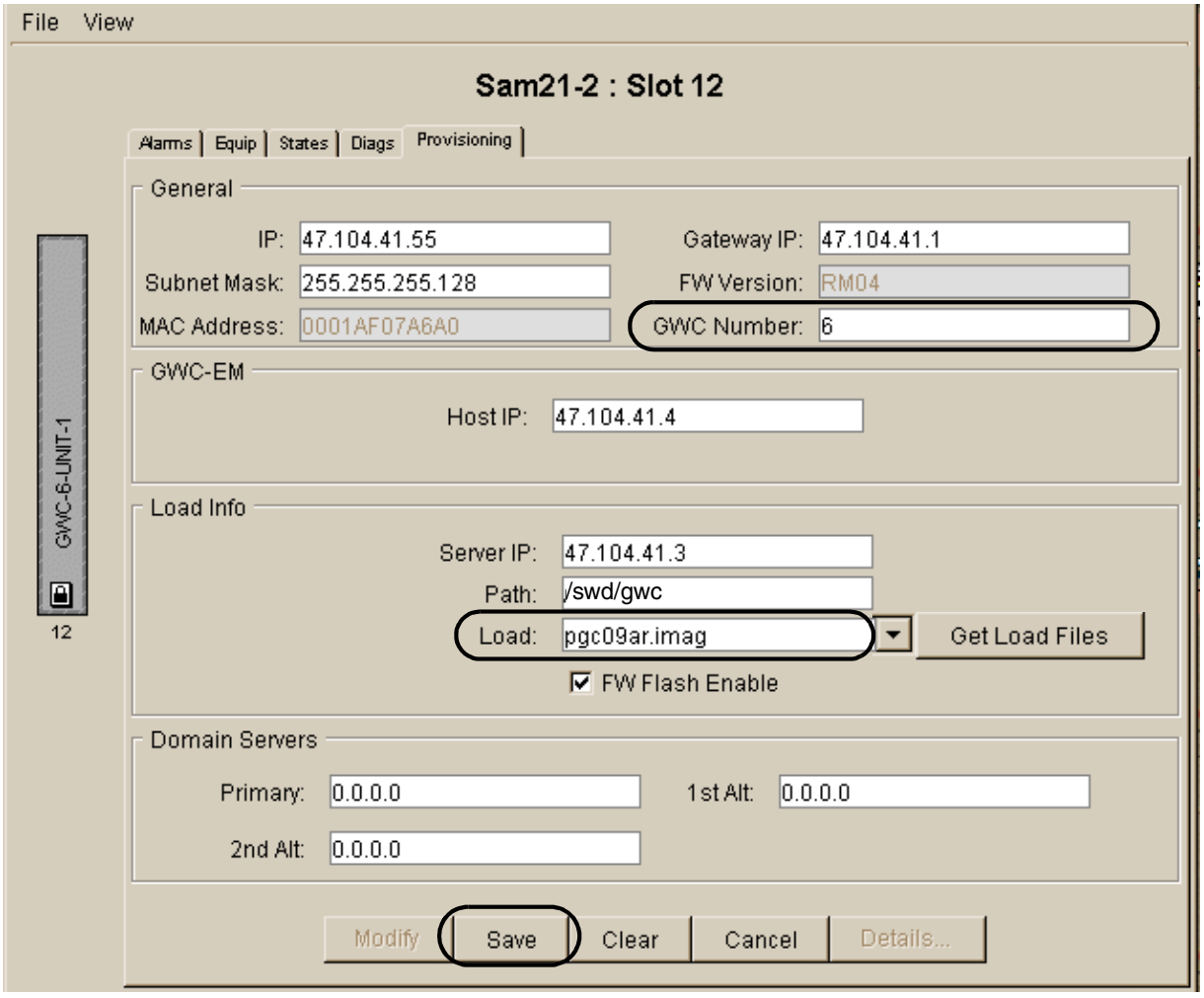
There is a requirement to enter the GWC number into this field which is used to label the GWC in the CS 2000 SAM21 Manager shelf view panel. This number is manually assigned and no error checking is performed to ensure it matches with the number in the CS 2000 GWC Manager. A number from 0 to 255 can 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 can 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

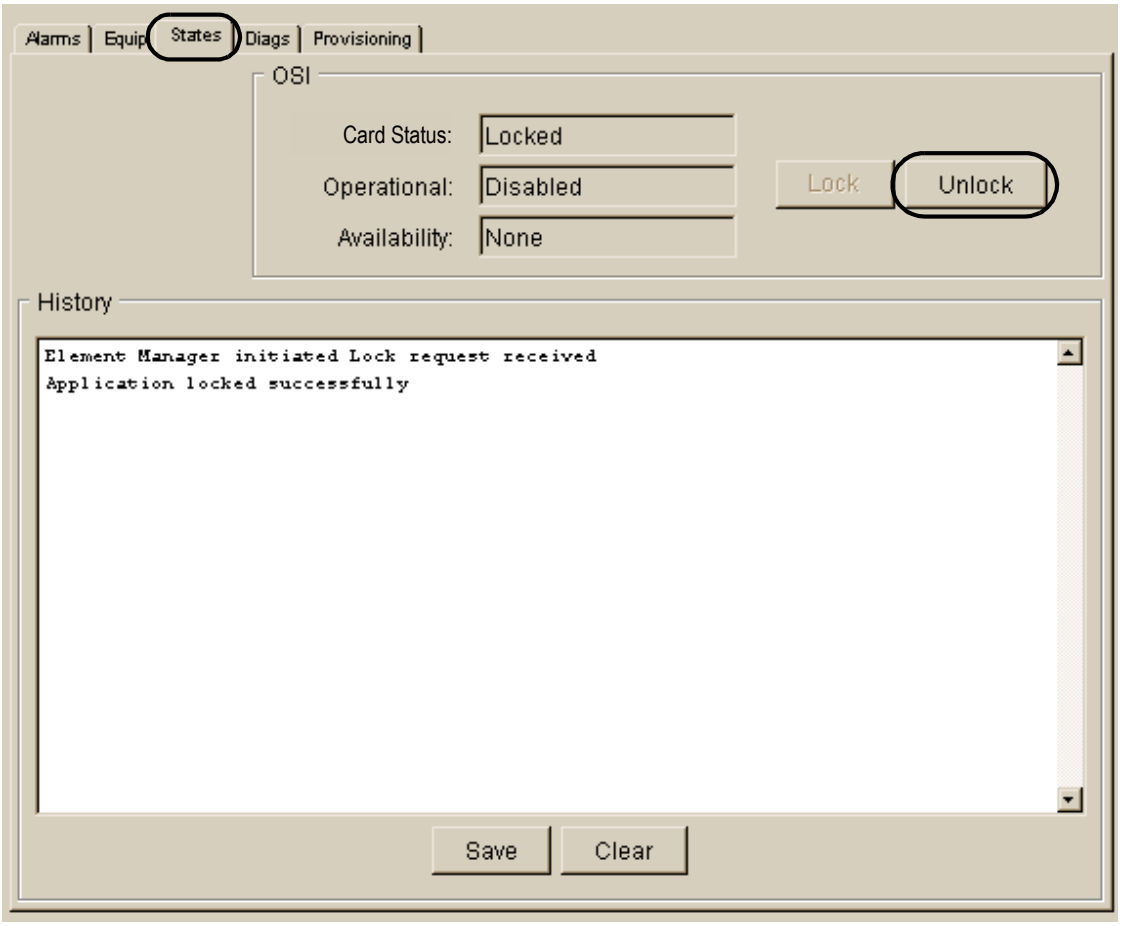
value given the cards in the CS 2000 GWC Manager as described in step 4 of this procedure.

13 Click the Save button.

If the load name or path name are incorrect, a Load Validation Failure message is displayed. You can choose to force the change or return to the provisioning panel to correct the error.



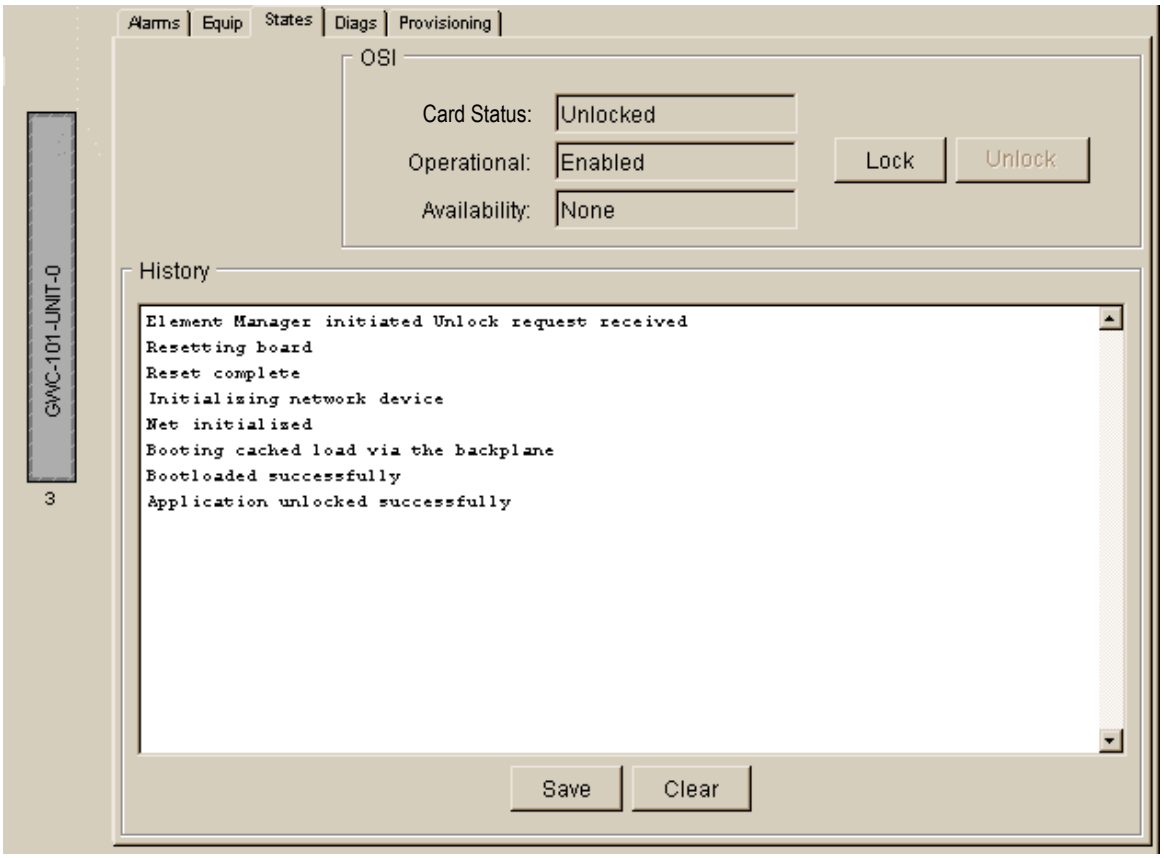
14 Click the States tab to display the status of the GWC card.



15 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 is automatically returned to service (RTS).

16 Observe the History display until the screen message: Bootloaded successfully appears.

If the card status does not display the message: Application unlocked successfully, then click the Lock button in the card view and wait for the message: Application locked successfully. Then, click the Unlock button again. If you are still unable to successfully unlock a GWC card, contact your next level of support.



At the CS 2000 GWC Manager

17 Use the following table to determine your next step.

If	Do
you are upgrading the first card in the seed GWC node, and there are patches that must be applied	go to step 18
otherwise	go to step 20

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

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

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.

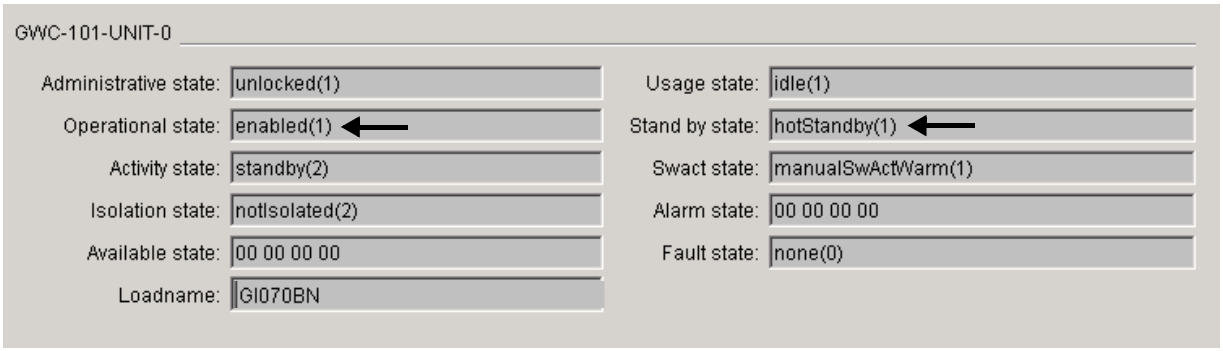
All necessary procedures, as well as the patching checklist and additional patching information, are available in the "Carrier Voice over IP Network patching" section of *Upgrading a Carrier Voice over IP Network*, NN10440-450.

Task	Procedure
Audit the GWC unit for existing patch activity.	"Performing a device audit using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
Retrieve the patch files from CD or electronically, and copy them into the NPM database.	"Transferring patches to the NPM database manually" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
If you wish, define reports for a GWC.	"Defining reports using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
Apply patches to the standby GWC unit.	"Applying patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
Activate the applicable patches.	"Activating patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
If required, deactivate any obsolete patches.	"Deactivating patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450
If required, remove any obsolete patches.	"Removing patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450

19 Take an image of the standby GWC unit using procedure Take a manual GWC software image on page 161.

20 Verify that the inactive GWC's Operational State is enabled and a standby state of hotstandby.

If the inactive GWC does not come into an enabled operational state of and a hotstandby state of, then refer to the section GWC does not RTS, in the procedure Troubleshoot GWC upgrades on page 176. If error recovery fails, stop this procedure and contact your next level of support.

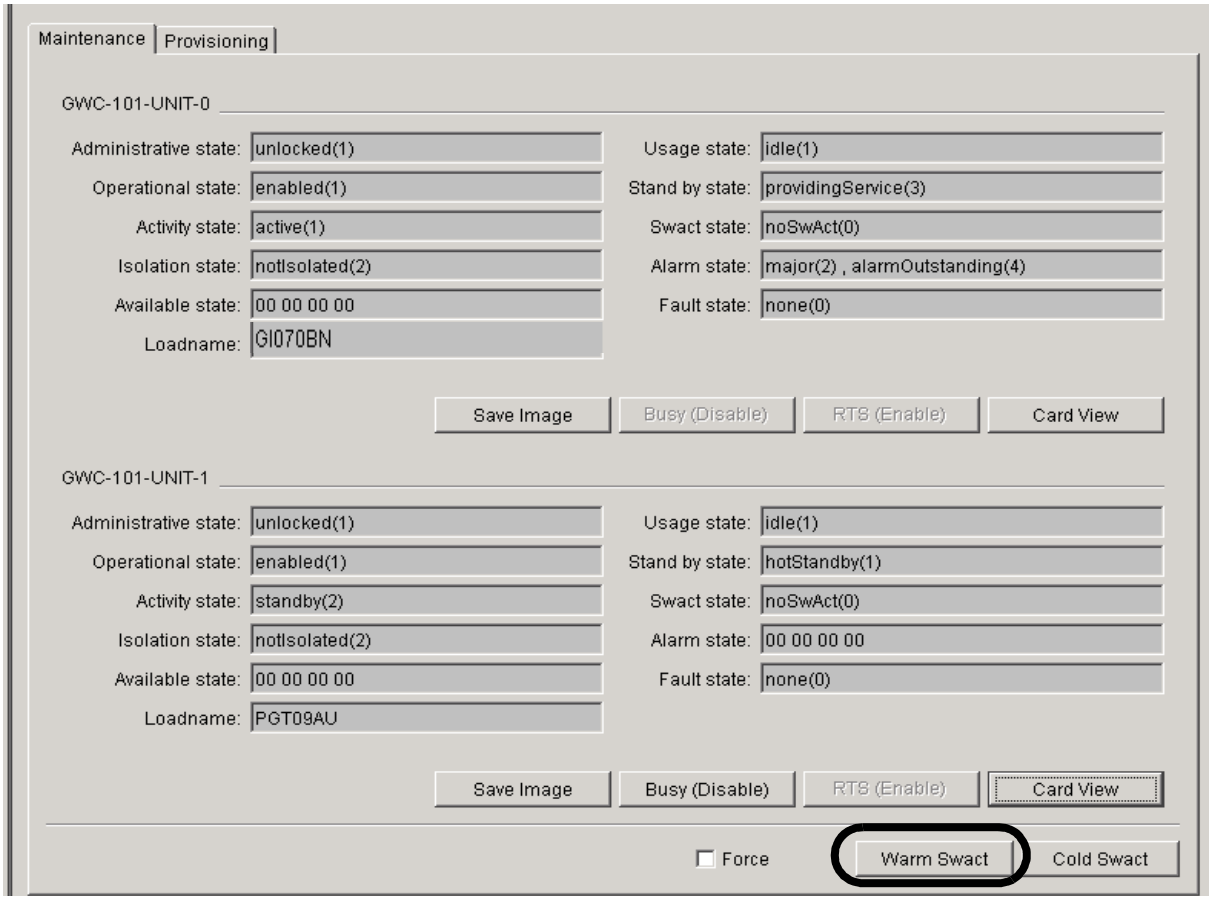


At the CS 2000 GWC Manager

21 Perform a Warm SwAct by clicking the Warm Swact button.

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 176.

If the GWC card does not successfully execute a warm SwAct using the Troubleshooting procedure, then perform the procedure Roll back a software upgrade on a standby GWC node on page 144.



22 Use the following table to determine your next step.

If	Do
you need to upgrade the mate GWC card (now the new standby GWC card) in the same node	go to step 3 and complete this procedure
you need to upgrade cards in another GWC node	go to step 2 and complete this procedure
all cards in all GWC nodes have been upgraded You only need to perform this procedure once for each card in each GWC node.)	go to step 23

23 You have completed this procedure. Return to Upgrading the GWC on page 10.

Roll back a software upgrade on a standby GWC node

Purpose of this procedure

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

CAUTION

Downgrades are only supported as part of backing out of the upgrade of an individual GWC type. Call survivability, as specified in this document, 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.

Restrictions and Limitations

The following restricts apply to using this procedure:

Rollbacks can occur only on a standby GWC card.

CAUTION

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

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.

Prerequisites

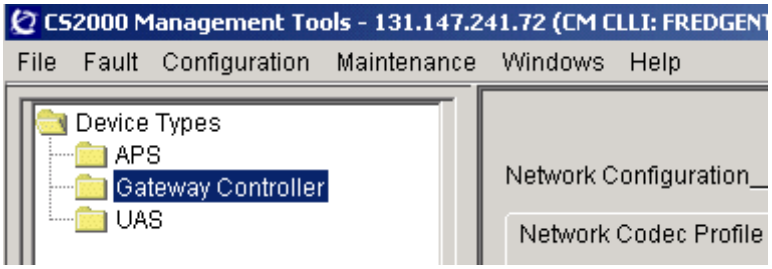
The following prerequisites apply to this procedure:

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

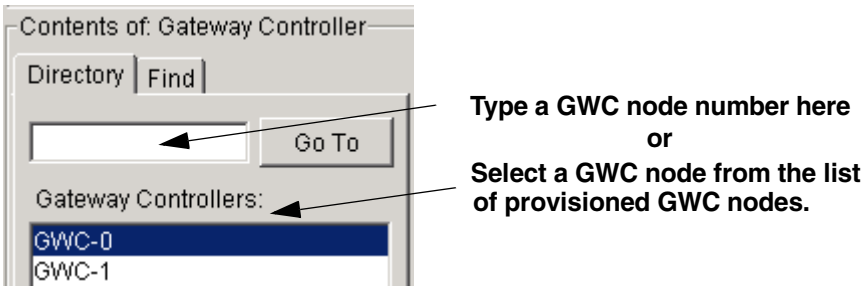
Action

At the CS 2000 GWC Manager client

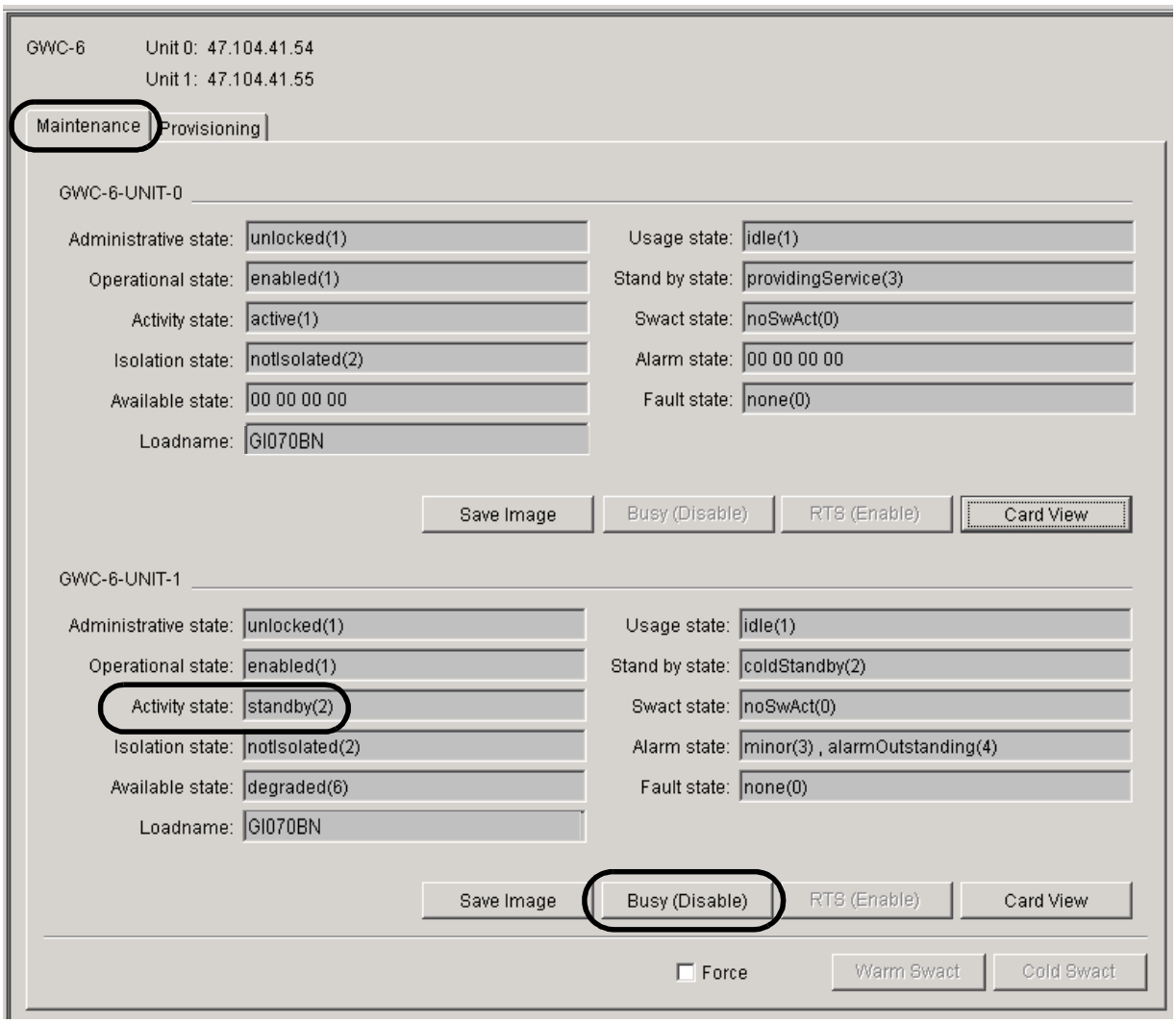
1 At the CS 2000 Management Tools window, click on the Gateway Controller folder from the Device Types directory tree in the far left frame.



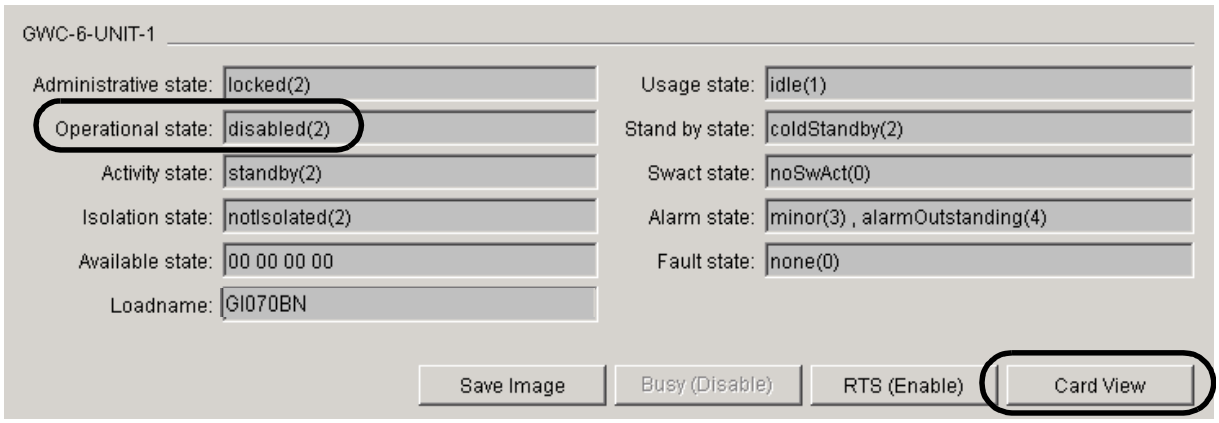
2 From the Contents of: Gateway Controller frame, select the appropriate GWC node you wish to roll back.



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

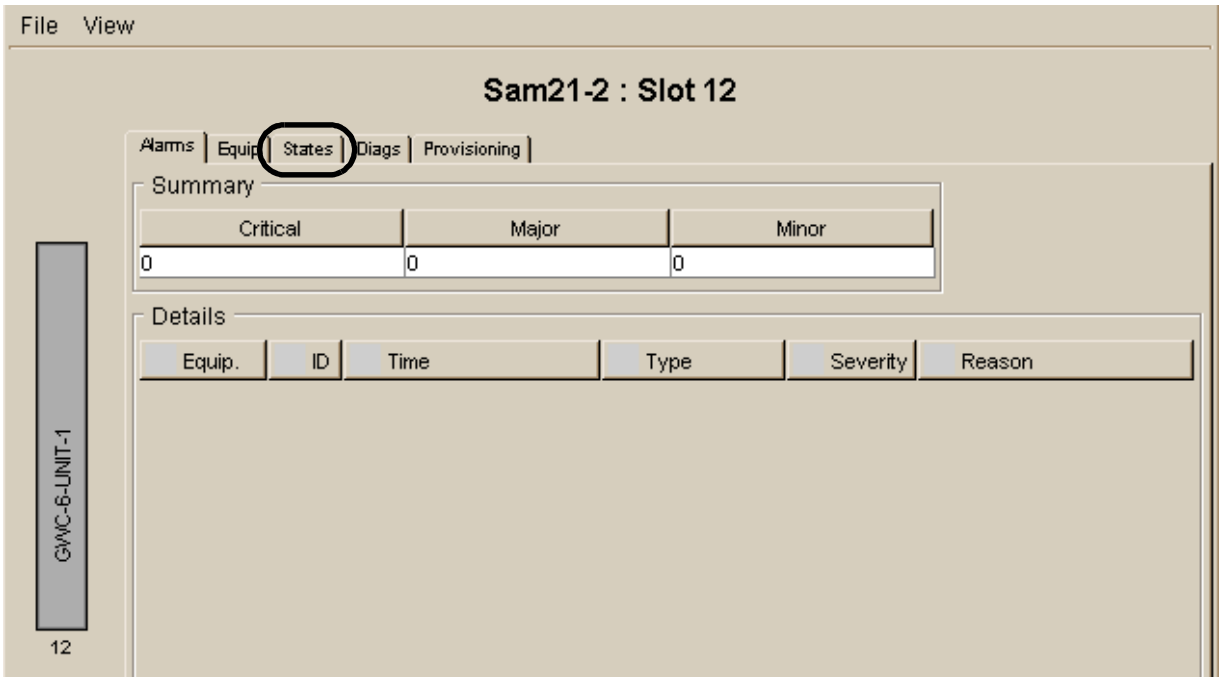


4 When the Operational state of the standby card is disabled, click the Card View button to access the card view. This action opens the CS 2000 SAM21 Manager.

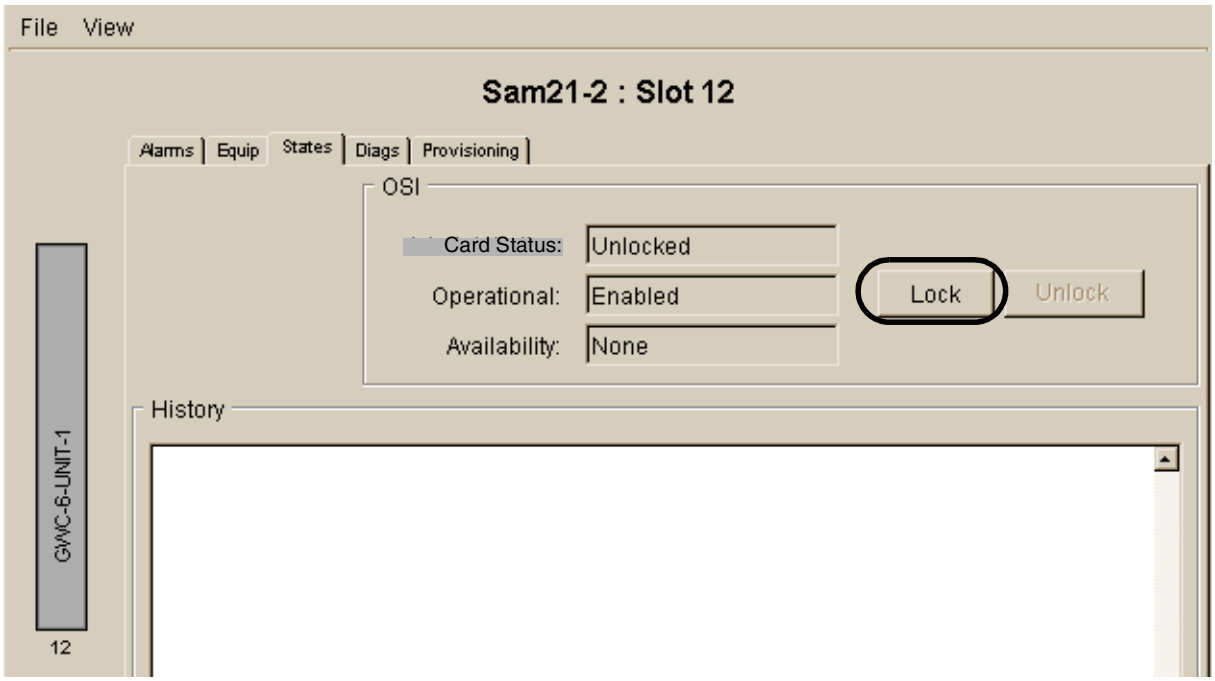


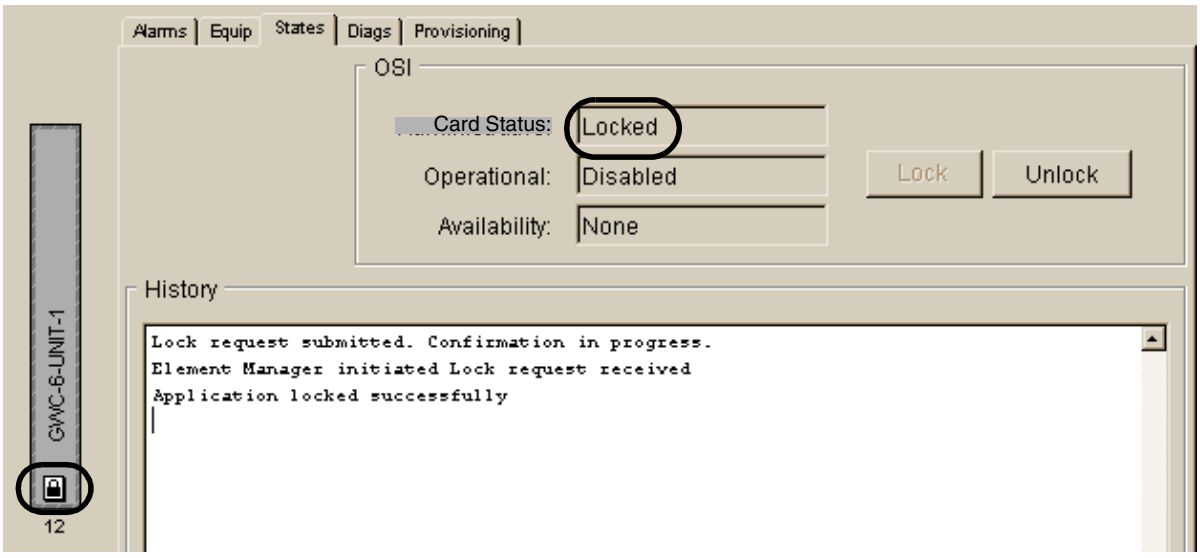
At the CS 2000 SAM21 Manager client

5 Select the States tab in the card view.

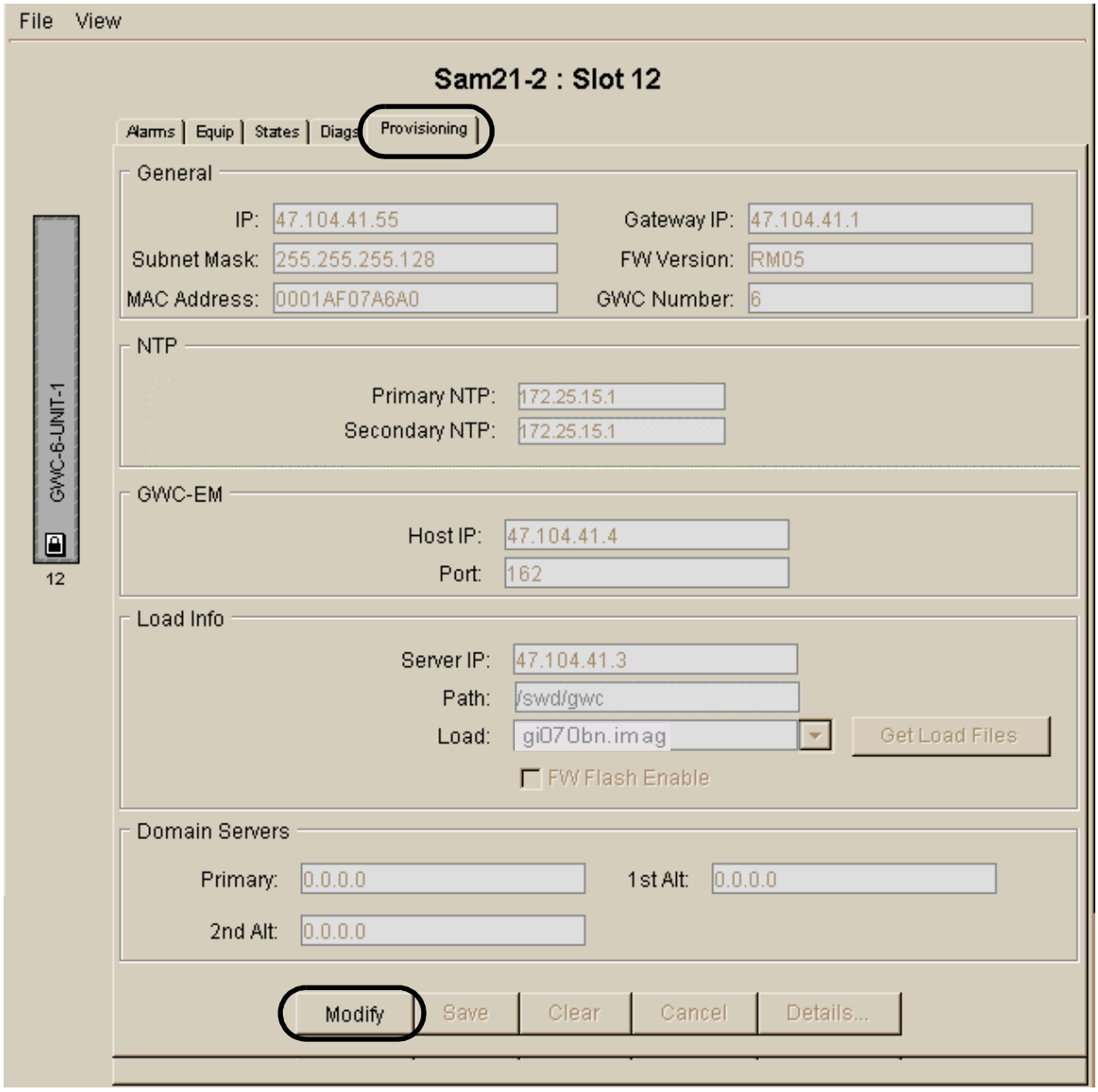


6 Click the Lock button to lock the card. Wait for the message in the History window indicating that the card is locked. Also, notice the lock icon on the card graphic at the left of the screen and the Card Status Locked.





7 Select the Provisioning tab in the card view.



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

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

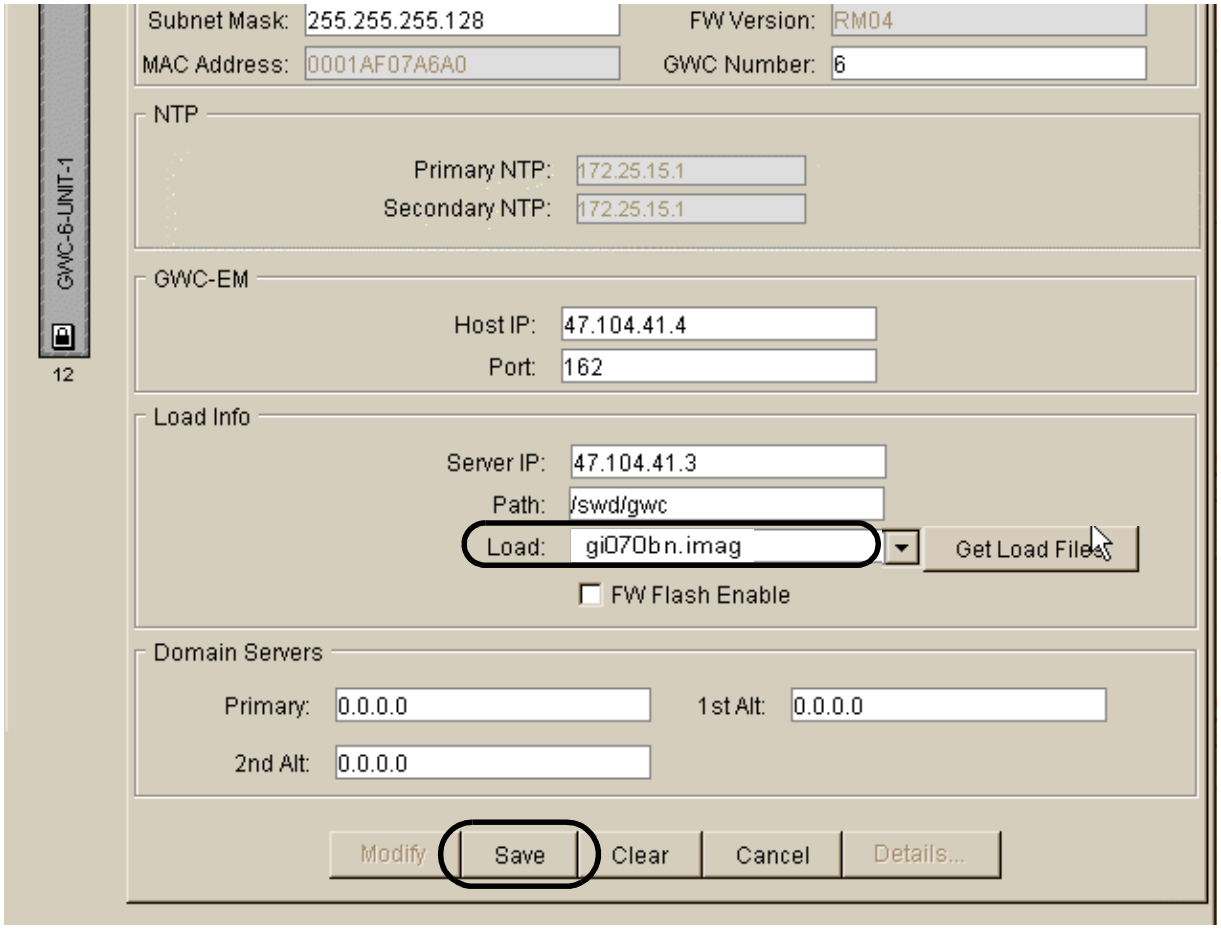
10 Click the Save button.

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

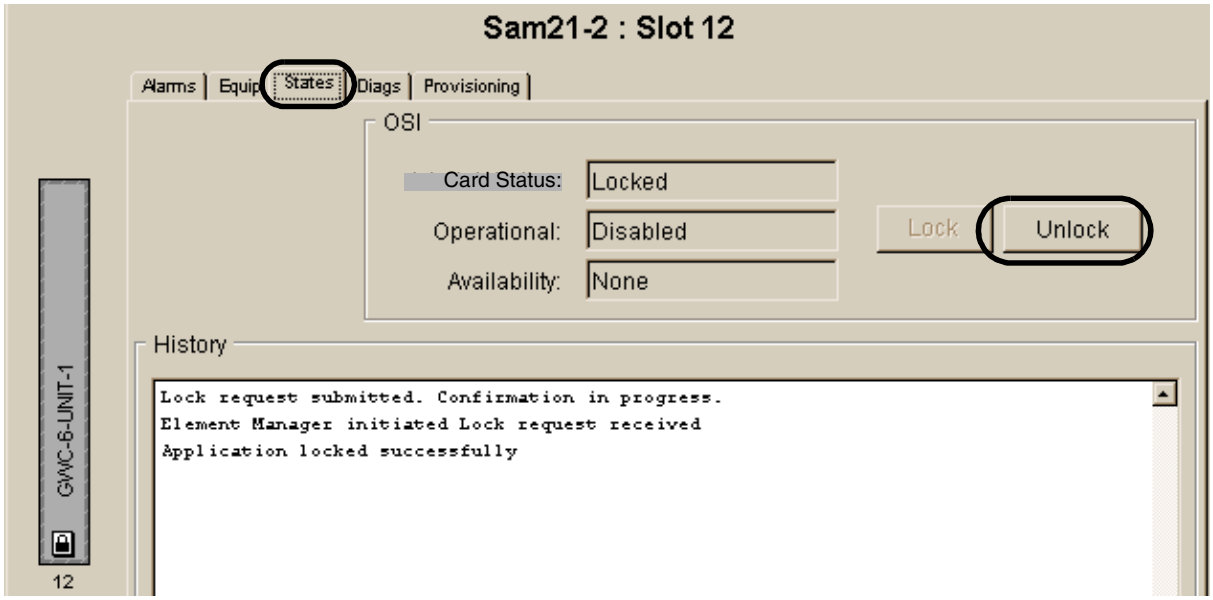
CAUTION

For CS 2000 Core Manager the Path: field must be set to /swd/gwc; For CBM the Path: field must be set to /gwc.

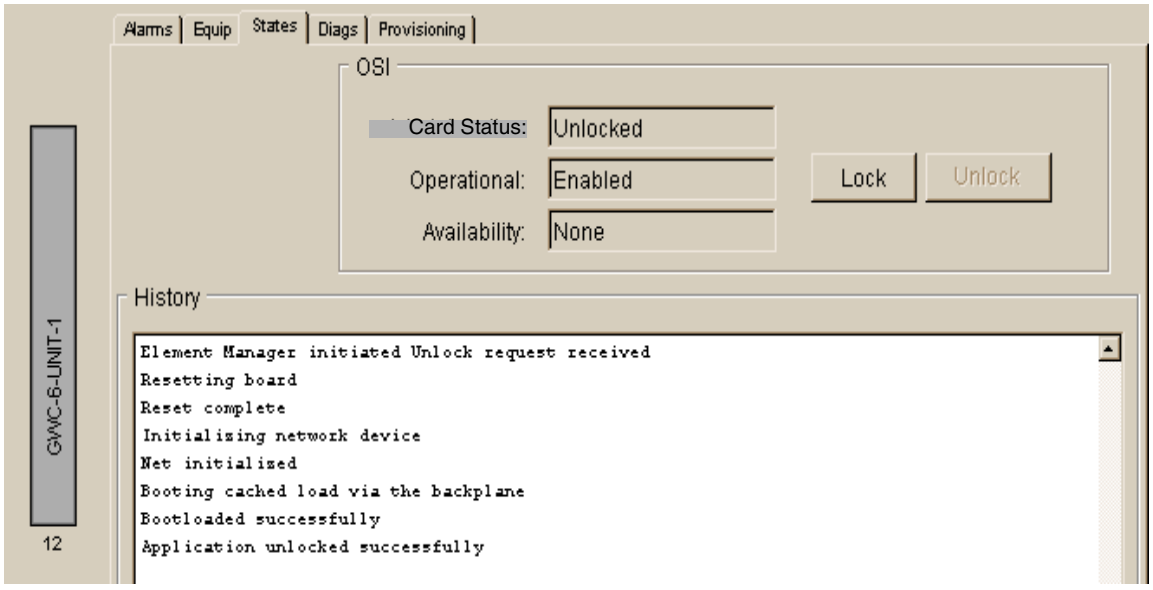
Other processes are tied to this directory. For example, the GWC load delivery software places the load in the /swd/gwc directory. Also, GWC auto-imaging is a network file system (NFS) mount of the /swd/gwc directory.



11 Select the States tab in the card view.



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



13 Use the following table to determine your next step.

If	Do
you are downgrading the first card in the seed GWC node, and there are patches that must be applied to the earlier software load. (The image file of the earlier software load already contains the required patches. The following steps to patch the load may not be required.)	go to step 14
otherwise	go to step 16

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

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

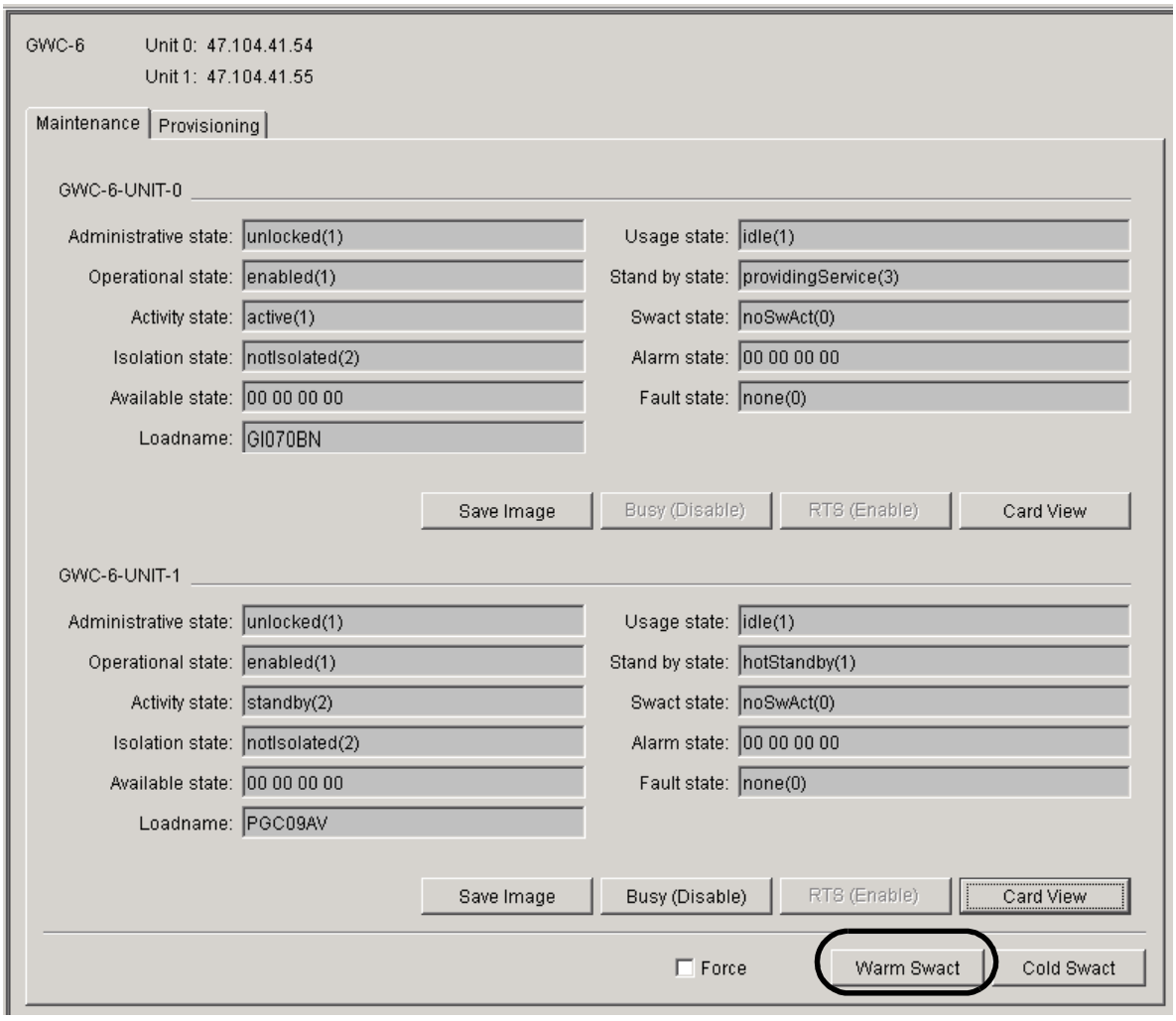
Task	Procedure
Audit the GWC unit for necessary patch activity.	"Performing a device audit using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.
If you wish, define reports for a GWC.	"Defining reports using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.
Apply patches to the standby GWC unit.	"Applying patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.
Activate the applicable patches.	"Activating patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.
If required, deactivate any obsolete patches.	"Deactivating patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.
If required, remove any obsolete patches.	"Removing patches using the NPM" in *Upgrading a Carrier Voice over IP Network*, NN10440-450.

15 Take an image of the standby GWC unit. Follow procedure Take a manual GWC software image on page 161.

At the CS 2000 GWC Manager client

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

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



18 Use the following table to determine your next step.

If	Do
you need to downgrade the mate GWC card (now the new standby GWC card) in the same node	go to step 3 and complete this procedure
you need to downgrade cards in another GWC node	go to step 2 and complete this procedure
all cards in all GWC nodes have been downgraded (You only need to perform this procedure once for each card in each GWC node.)	go to step 20

19 Return to step 2, and repeat this procedure for each GWC node until all units in each node are rebooted from the new image, otherwise continue to the next step.

20 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Firmware flash a GWC card

Purpose of this procedure

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

When to use this procedure

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

Note: This procedure flashes the firmware on the GWC card only if the version of the firmware on the CS 2000 Core Manager or CBM is different from the firmware version on the card. If you need to flash the firmware on a card that contains the same version of the firmware as the CS 2000 Core Manager or CBM, then refer to Force a firmware flash of a GWC card on page 165 in this NTP.

Prerequisites

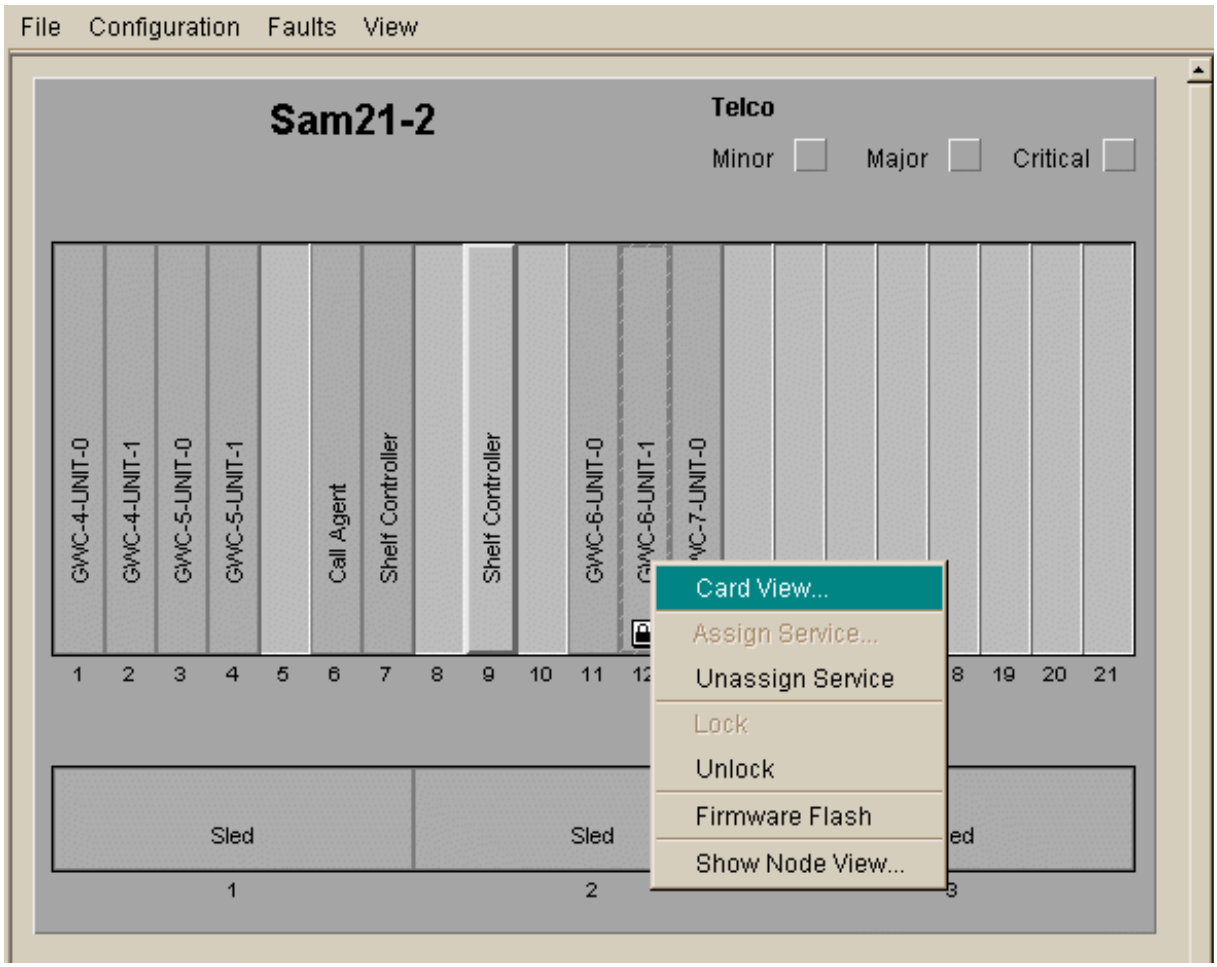
The GWC card you wish to flash must first be locked. Refer to the procedure “Lock a GWC card” in the *Gateway Controller Security and Administration* NTP, NN10213-611.

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

Action

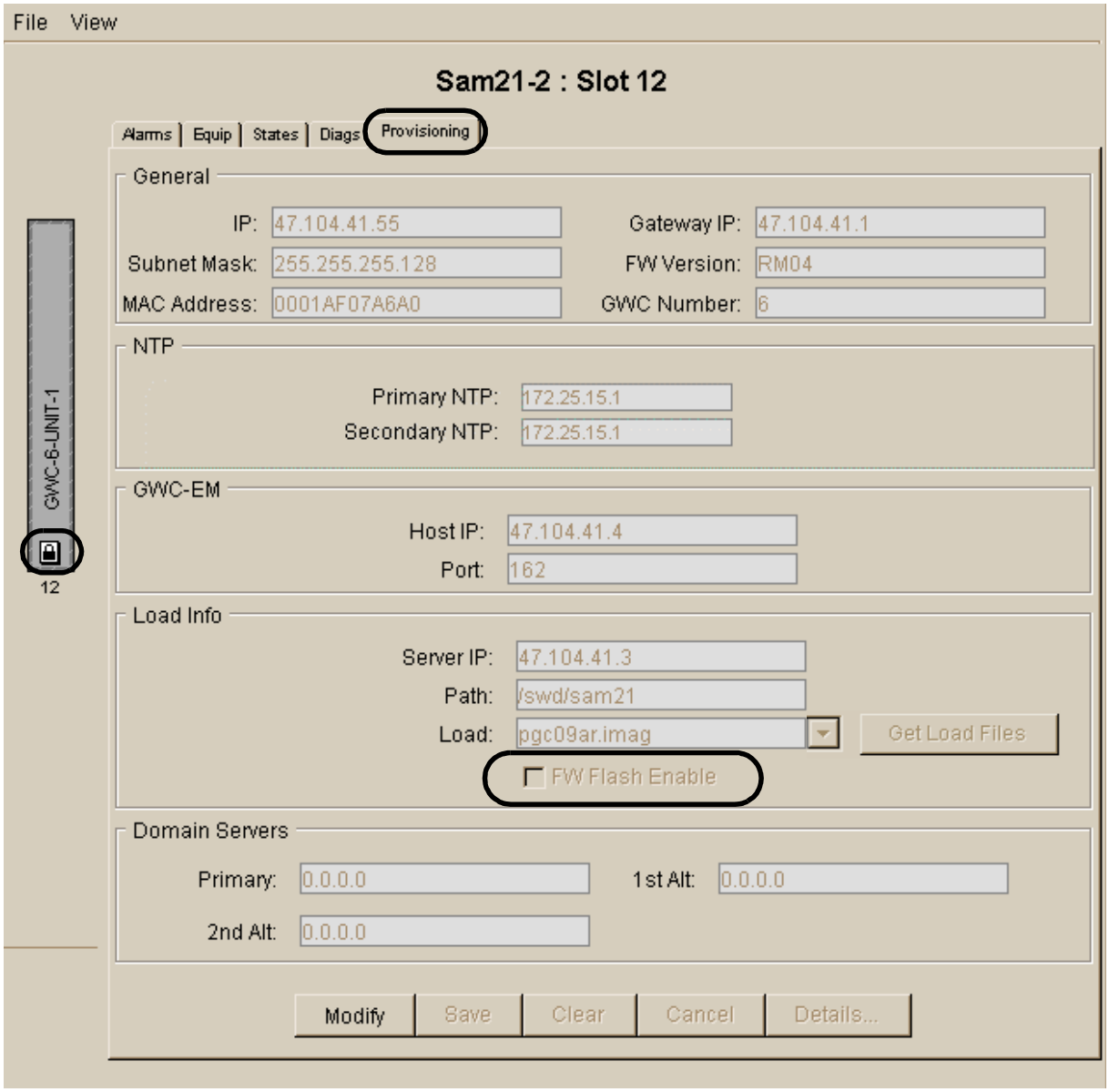
At the CS 2000 SAM21 Manager client

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.

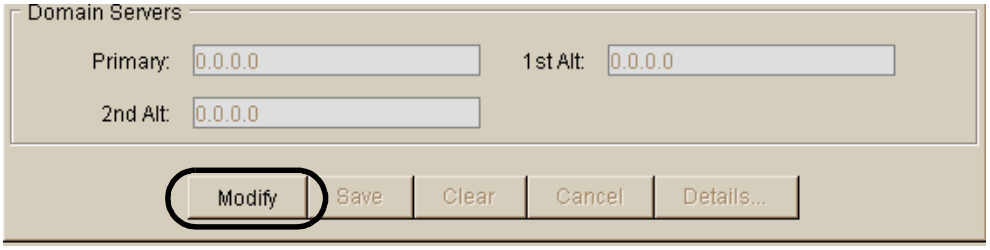
The lock icon is displayed on the card graphic at the left of the screen. This indicates that the card is locked.



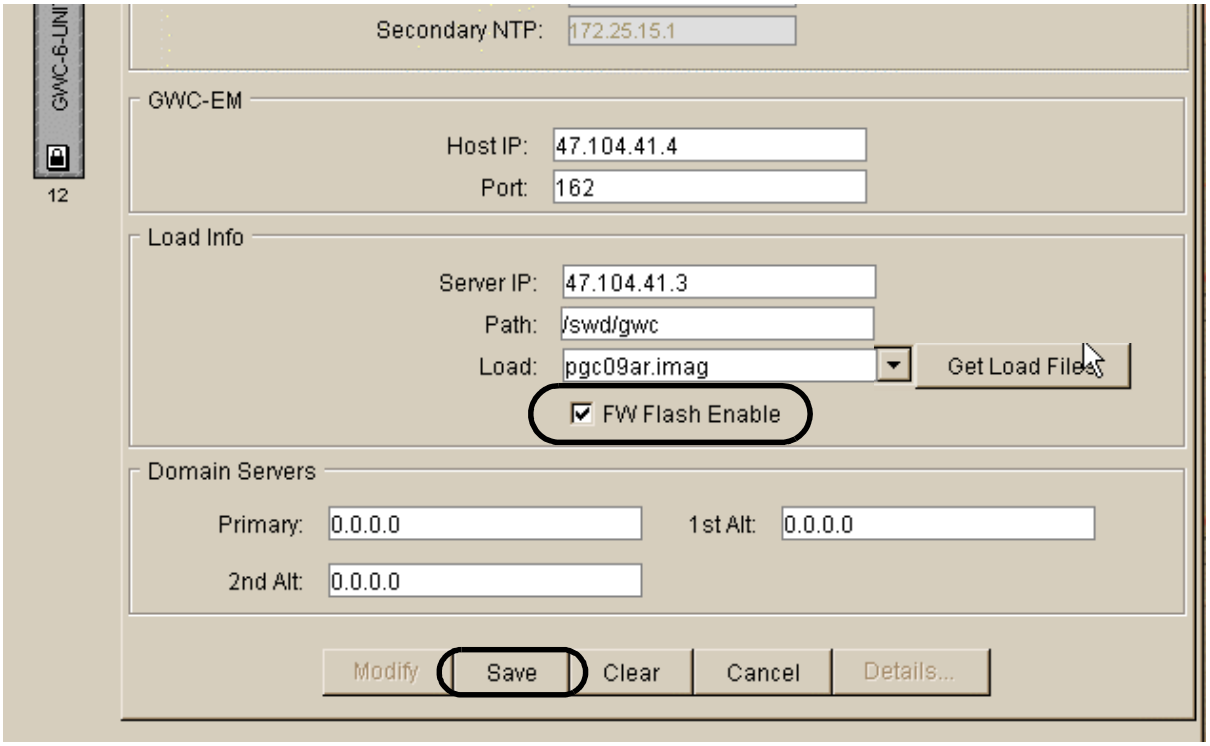
3

If	Do
If the FW Flash Enable checkbox is already selected and a new firmware version is available, the firmware flash process has already been started.	Skip to step 7.
If the Firmware Flash Enable checkbox is not selected,	continue with step 4.

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



5 Select the FW Flash Enable checkbox.

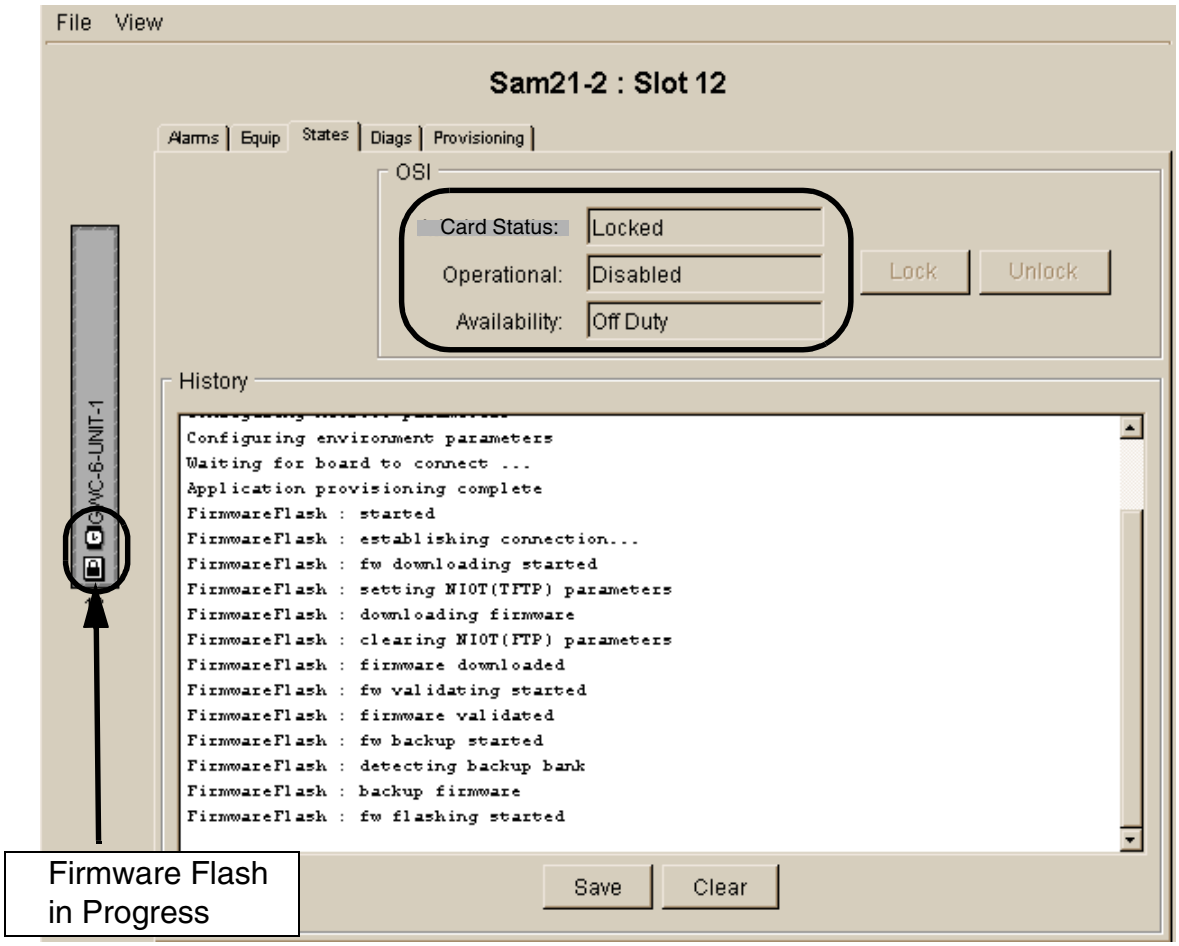


6 Click the Save button at the bottom of the screen.

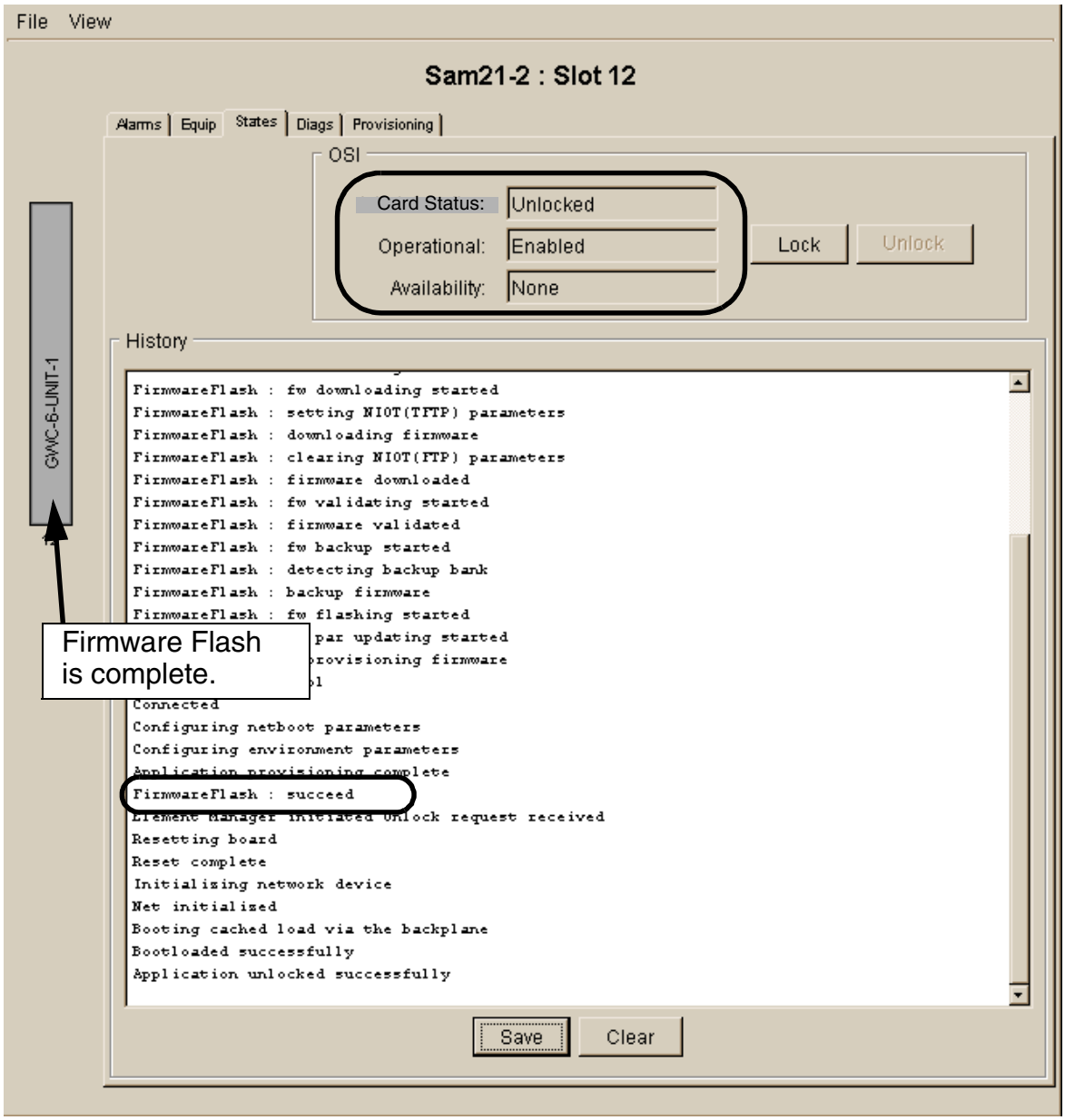
Firmwareflashing begins immediately.

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 transitions from locked-disabled-none to locked-disabled-off duty. Observe the various firmware flash progress messages in the History window. (Your messages can vary from those shown in the following graphic.)



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



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

10 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

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 or Core and Billing Manager (CBM).

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 173.

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

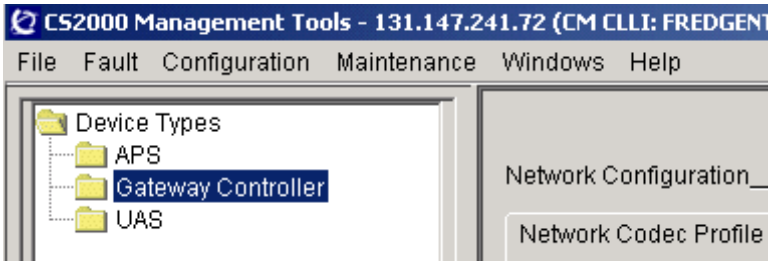
3 Copy the existing GWC software load file to a backup.

Example
 # cp pgc06as.imag pgc06as.imag.bak

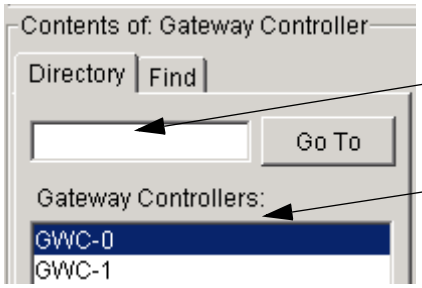
Note: You can use any name for the backup file name.

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 want to take an image.



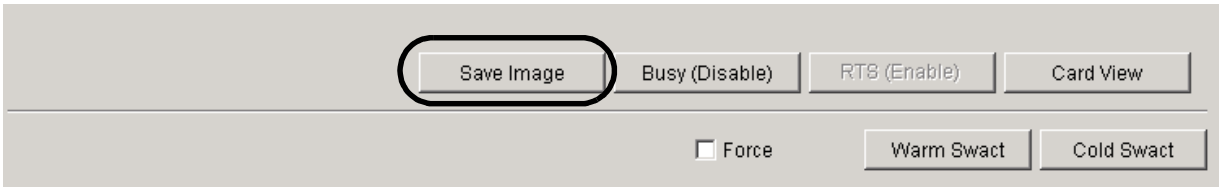
6 Select the Maintenance tab to view the Maintenance panel.

7 In the Maintenance panel, identify the GWC card in the node that has an upgraded load already installed. Click the Save Image button for that card to save the software image back to the CS 2000 Core Manager or CBM.

The Save Image command overwrites the existing GWC software load file on the CS 2000 Core Manager or CBM.

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

ATTENTION

If the load file name is a link on the file system, the link is replaced with a file of the same name. Nortel does not support using links to load files.

9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure. To return to the Overall GWC upgrade procedure, refer to Overall GWC upgrade process - manual on page 106. To return to the Overall GWC downgrade procedure, refer to Roll back a software upgrade on a standby GWC node on page 144.

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 Log out of the CS 2000 Core Manager or CBM.

5 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

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 stored on the CS 2000 Core Manager or Core and Billing Manager (CBM). This procedure forces firmware flashing of a GWC card even when the CS 2000 Core Manager or CBM and the GWC card have the same firmware version.

If you use the procedure Firmware flash a GWC card on page 155, you will not be able to flash a GWC card's firmware if it has the same firmware version as the CS 2000 Core Manager or CBM.

When to use this procedure

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

Prerequisites

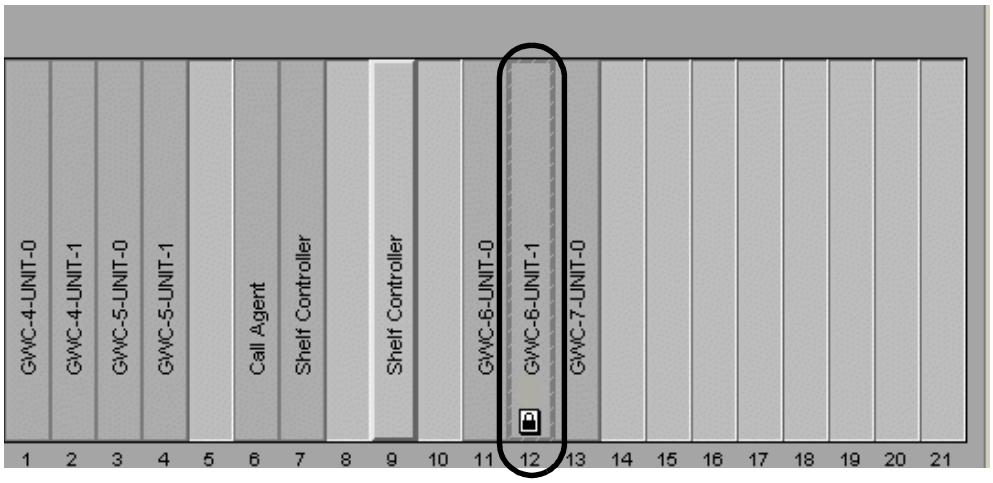
The GWC card you wish to flash must first be locked. Refer to the procedure "Lock a GWC card" in *Gateway Controller Security and Administration*, NN10213-611.

Action

At the CS 2000 SAM21 Manager client

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

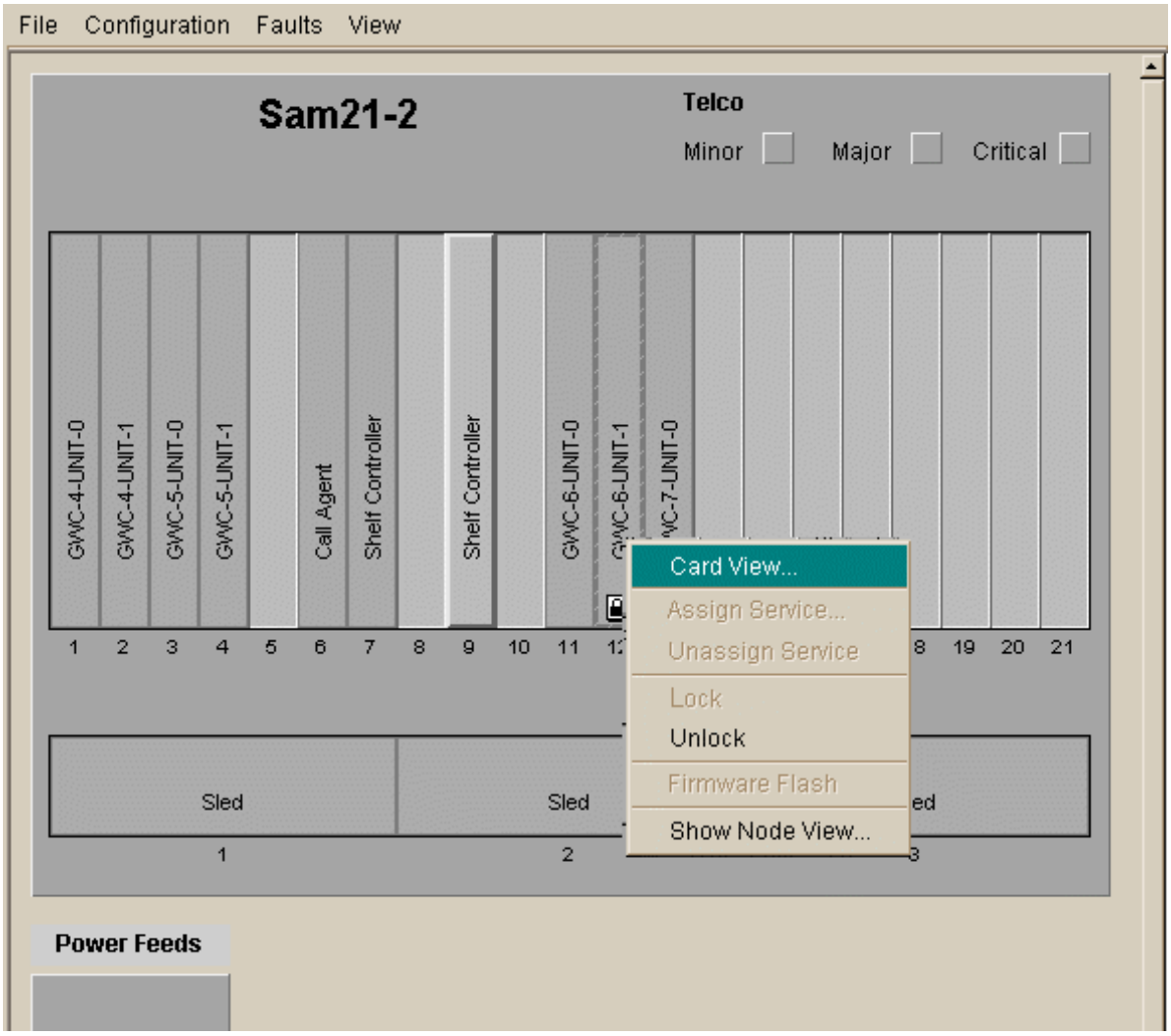
If you have recently locked the card using the Card View, click on the View menu and select Shelf View to verify the card status.



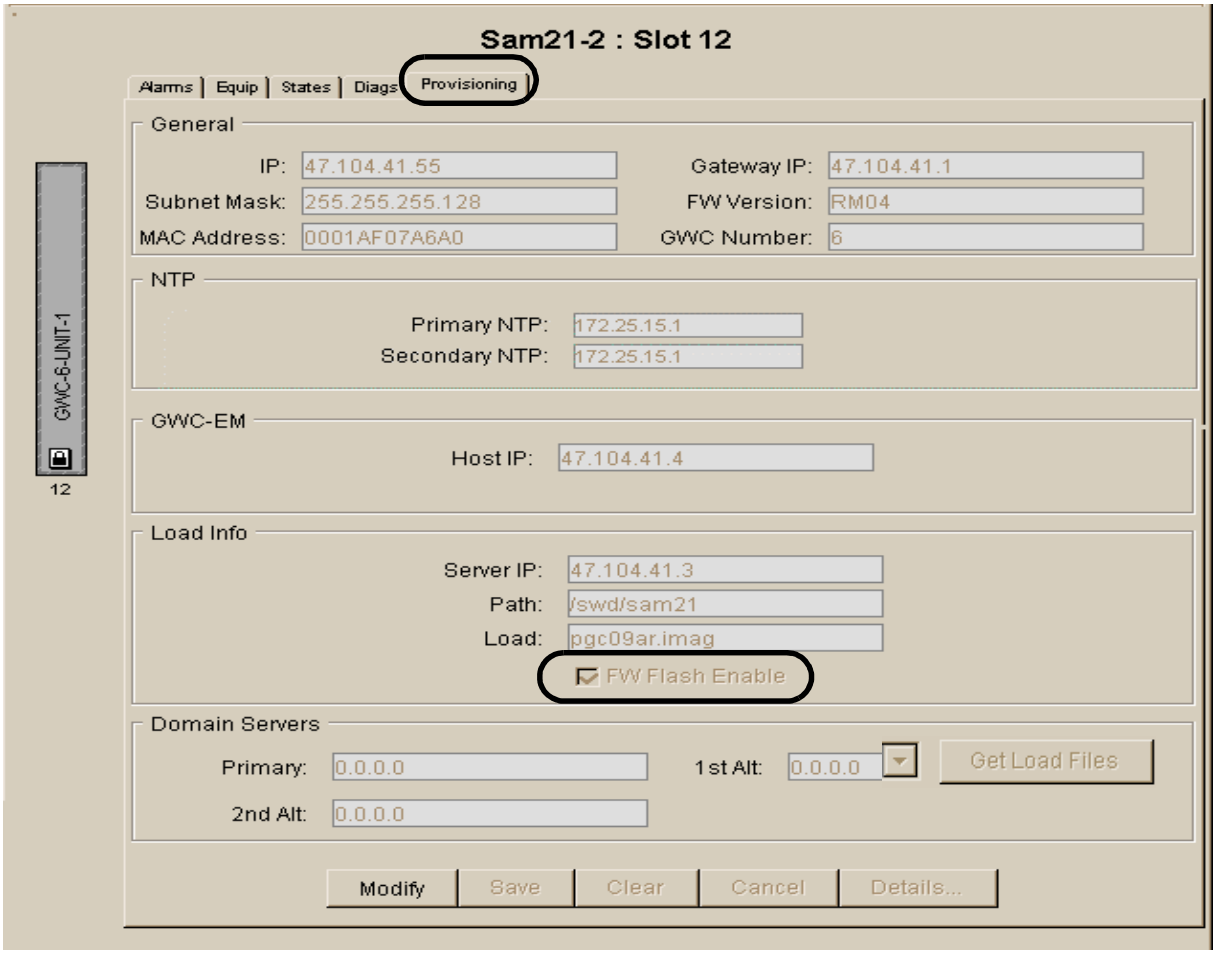
2 From the Shelf View window, right-click on the GWC card scheduled for flashing and determine your next action.

If	Do
If the Firmware Flash option is available	skip to step step 10
If the Firmware Flash option is not available (the text is faded in the 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.

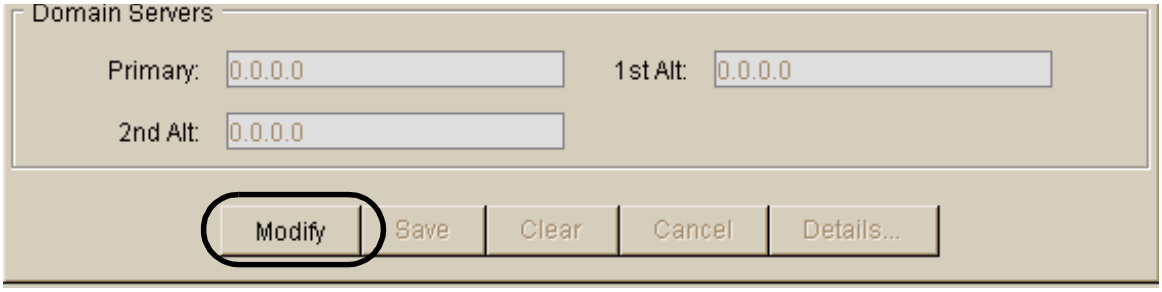


5 In the Provisioning panel, observe whether the FW Flash Enable check box is selected (checked). You cannot force a firmware flash if this option is selected.

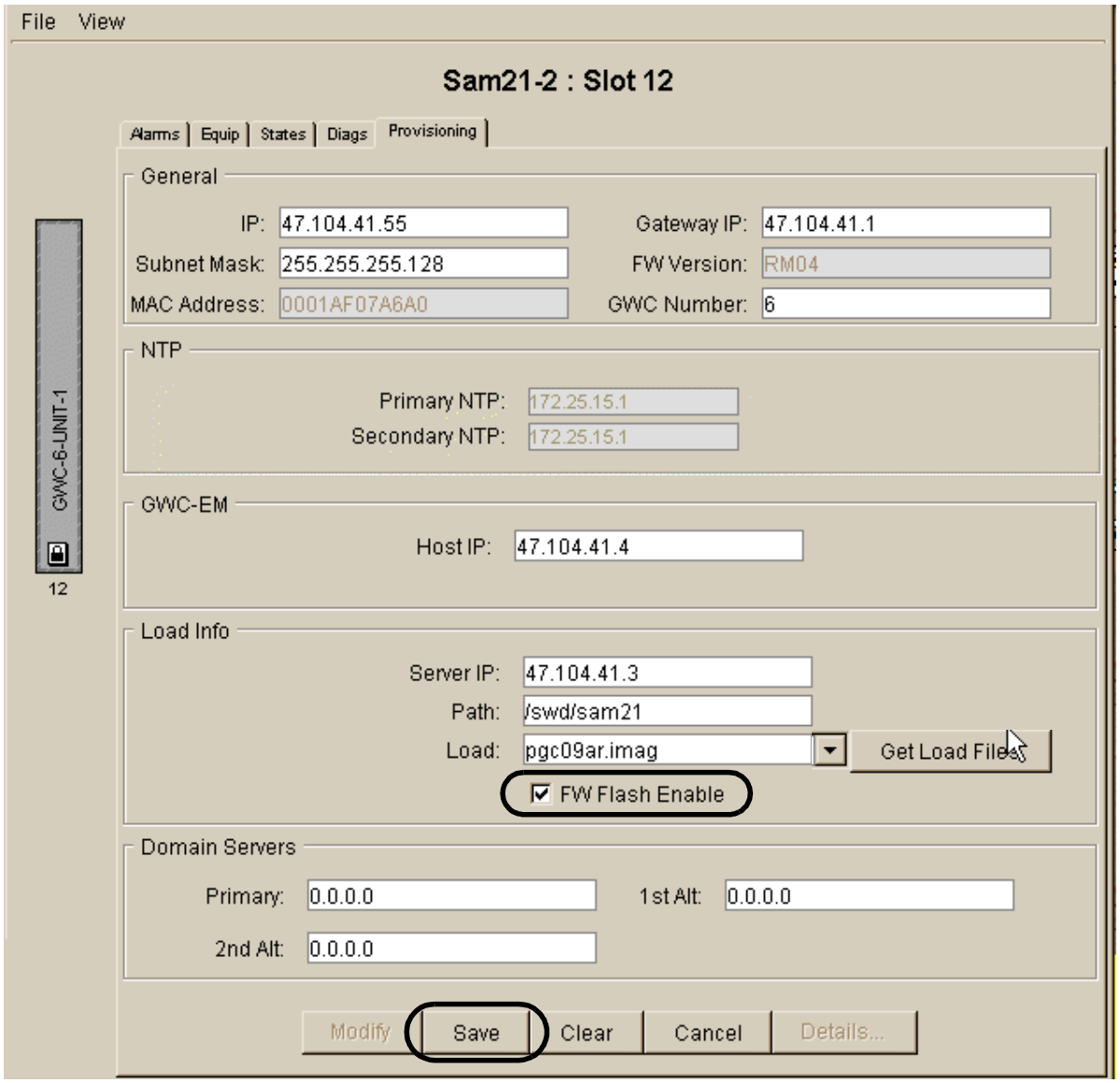
6 Use the following table to determine your next action.

If	Do
FW Flash Enable check box is selected	continue with step 7
FW Flash Enable check box is selected	go to step 10

7 In the Provisioning panel, click the Modify button.

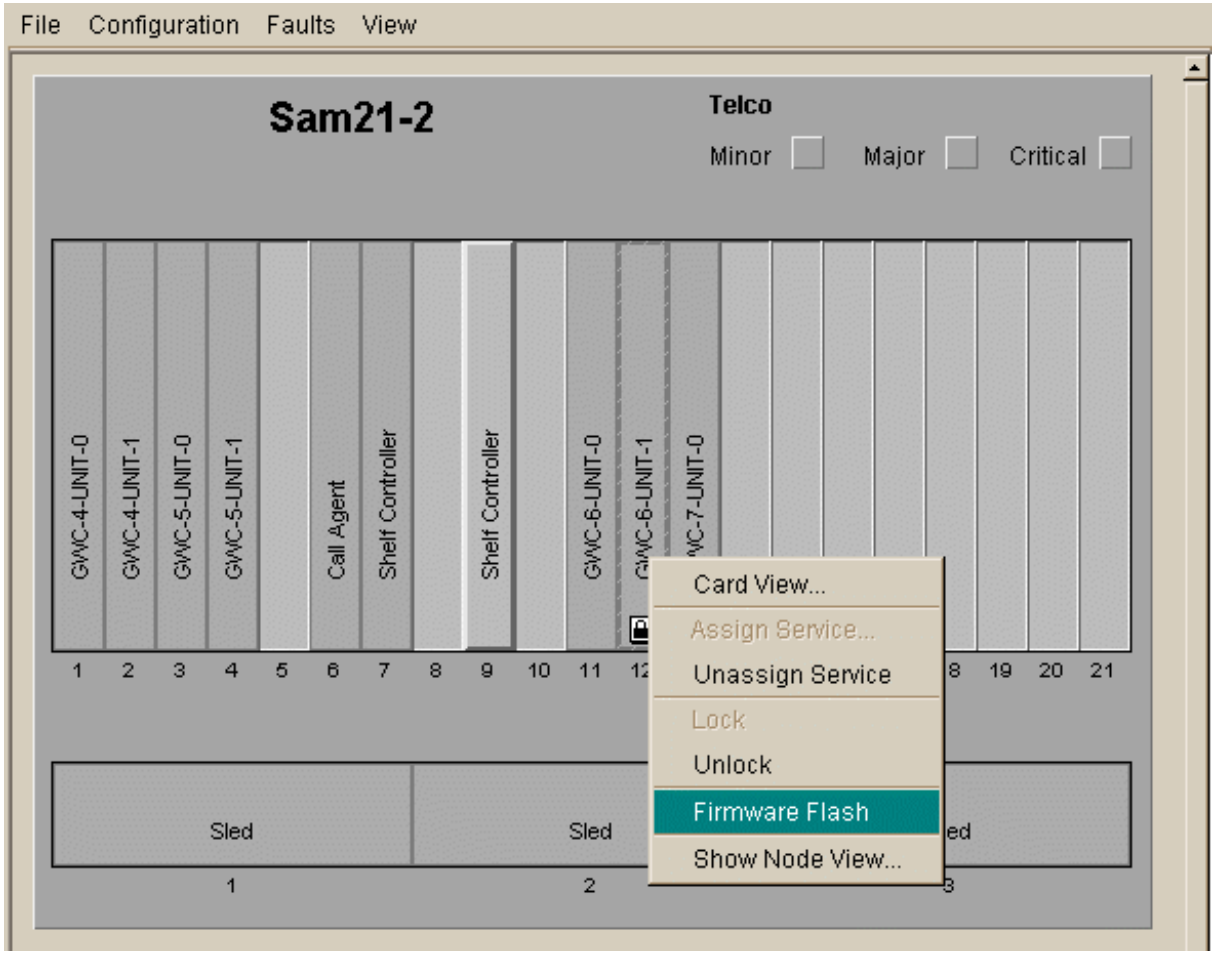


8 In the Provisioning panel, deselect the FW Flash Enable check box.



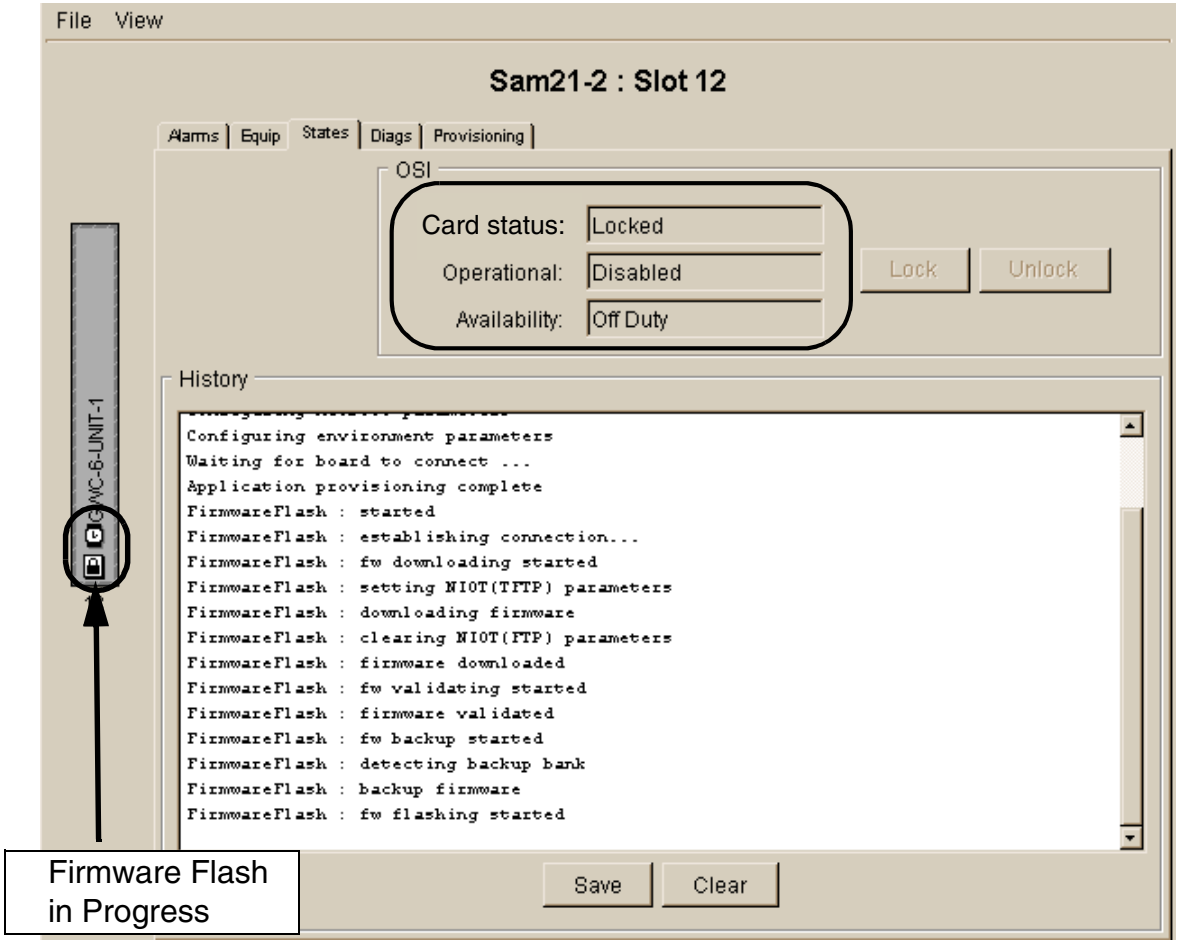
9 Click the Save button at the bottom of the screen to save the provisioning change.

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

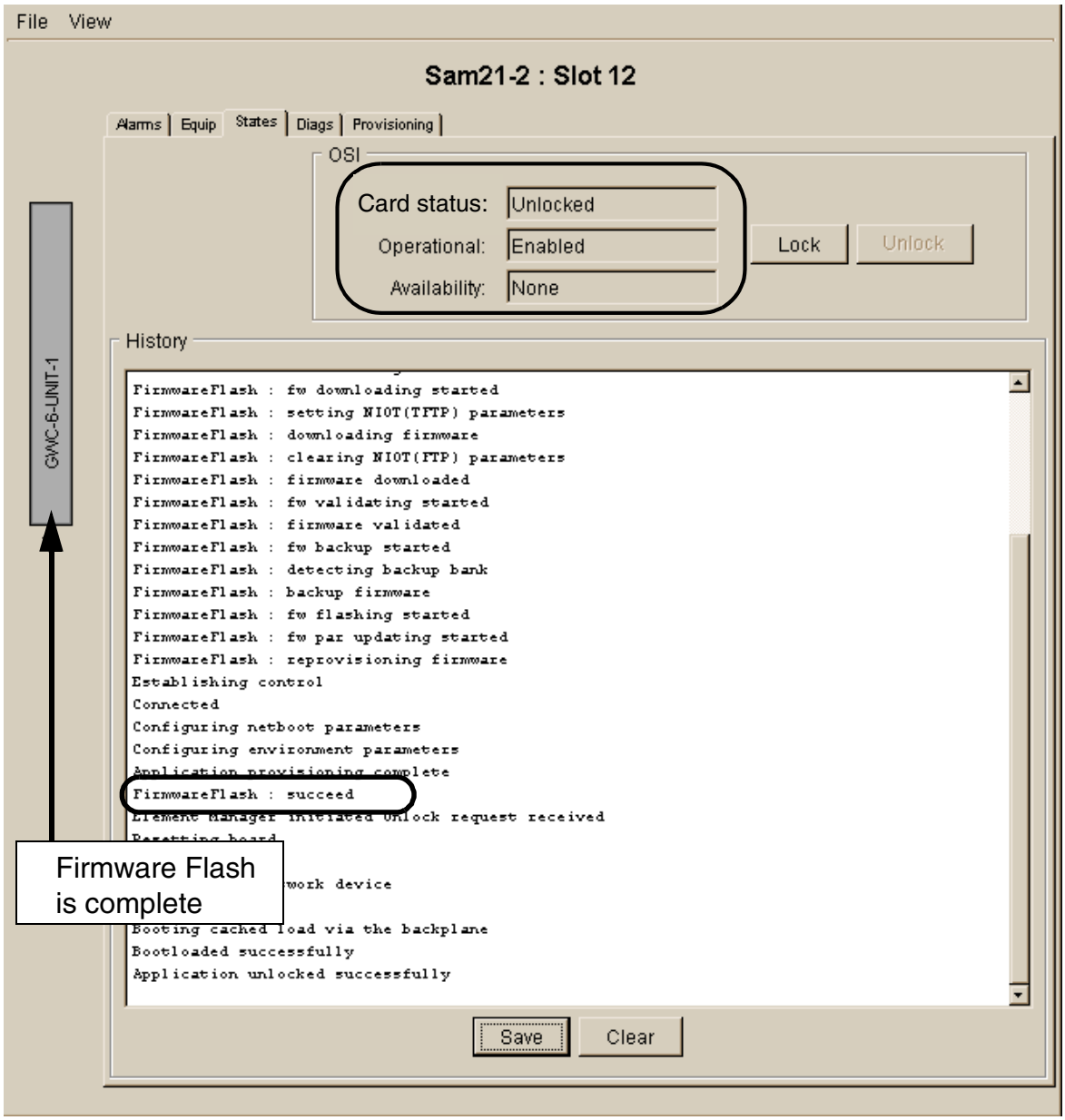


11 Select the States tab in the card view.

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 can vary from those shown in the following graphic.)



12 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.



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

14 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Enable or disable GWC software auto-imaging

Purpose of this procedure

Use this procedure to enable or disable the auto-imaging of a GWC software load. Auto-imaging provides a mechanism to automatically save up-to-date images of GWC software loads once daily on the CS 2000 Core Manager or Core and Billing Manager (CBM).

Auto-imaging is not designed for an office in which different patches are applied to GWCs using the same load. Instead, a procedure exists for taking a manual GWC software image. Refer to Take a manual GWC software image on page 161.

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.

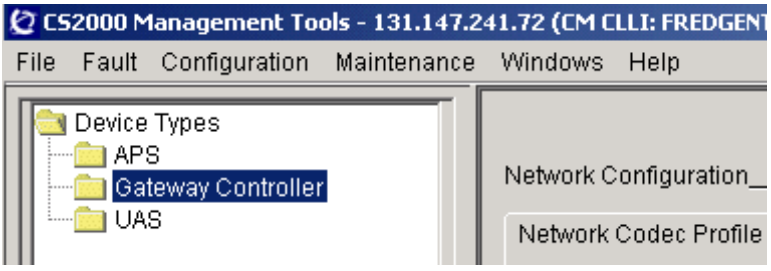
Prerequisites

This procedure has no prerequisites.

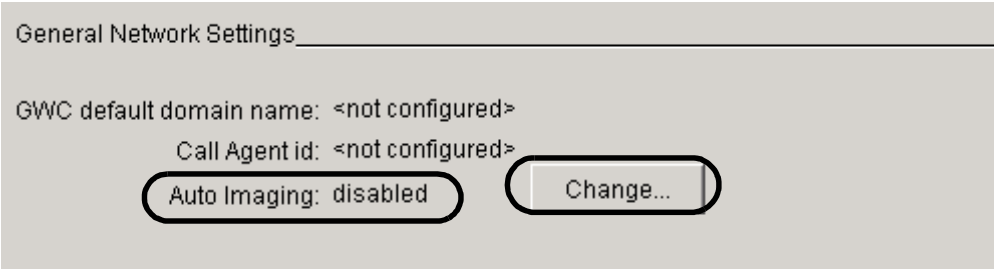
Action

At the CS 2000 GWC Manager client

1 Select Gateway Controller from the Device Types menu.



2 Locate the current status of Auto Imaging in the General Network Settings area, near the bottom of the main screen. Determine if the status is enabled or disabled.

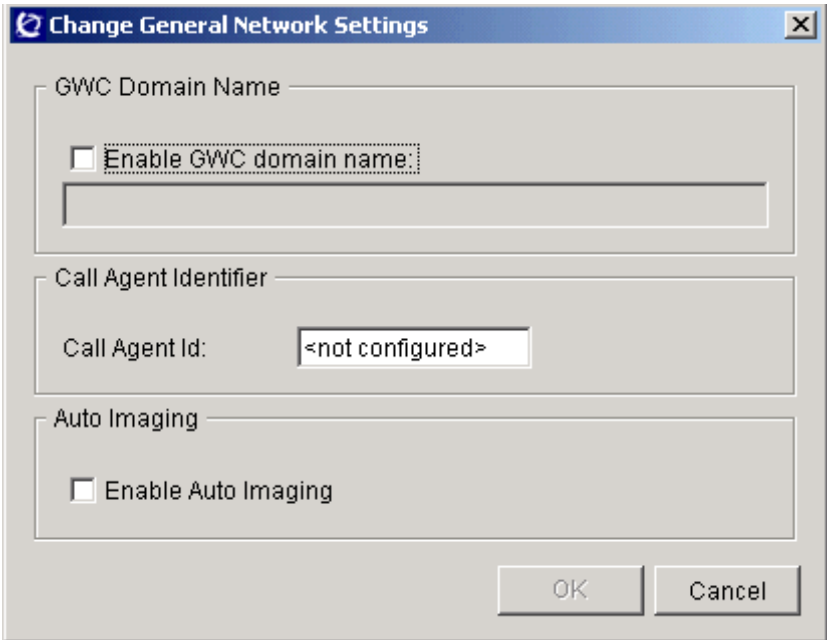


See the following procedures for information on the configuring the other network settings:

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

3 Click the Change button to change the status of auto imaging.

The Change General Network Settings dialog box is displayed.



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

5 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.

6 Click OK at the message to confirm the change.

7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

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.

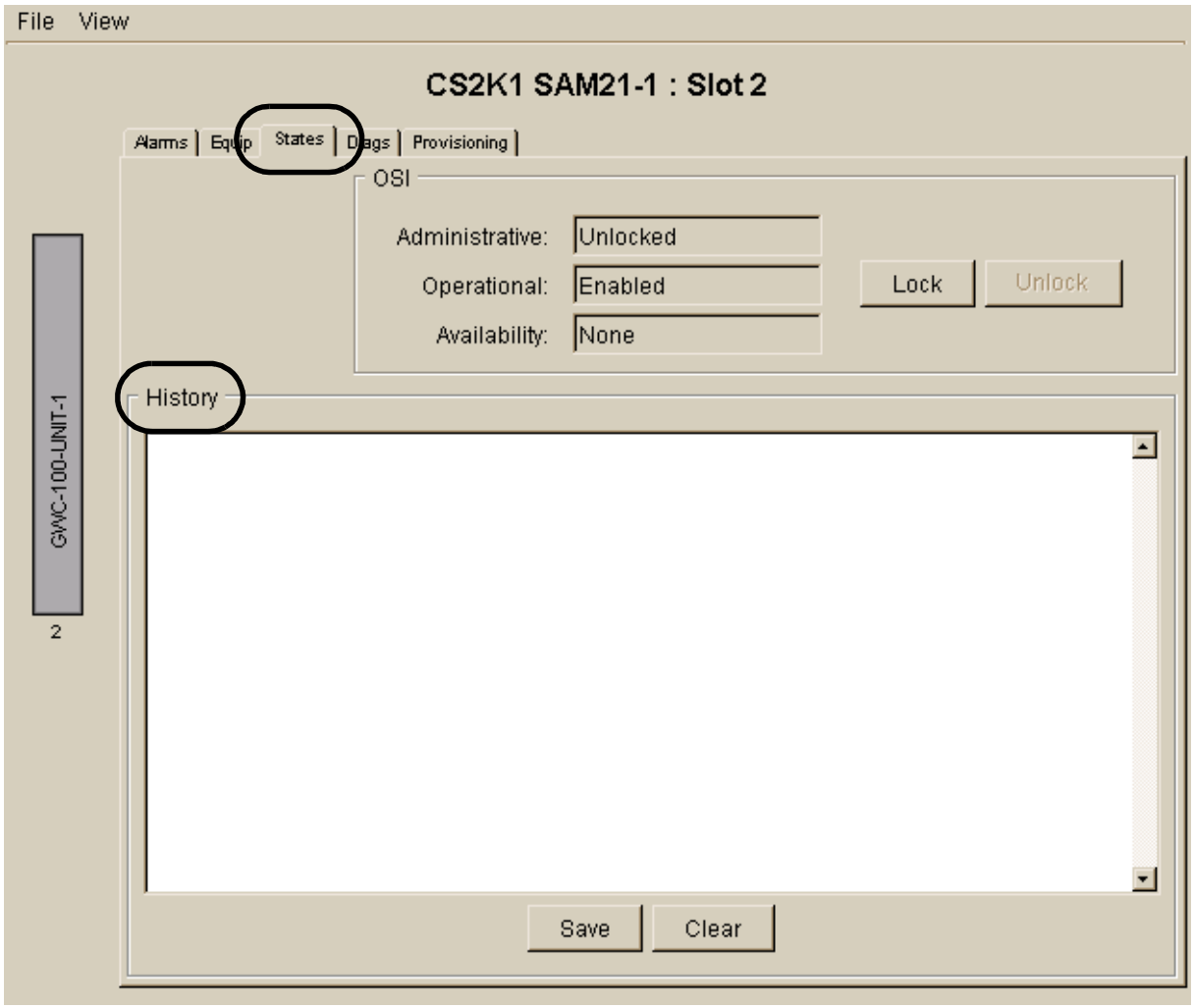
GWC does not RTS

At the CS 2000 SAM21 Manager client

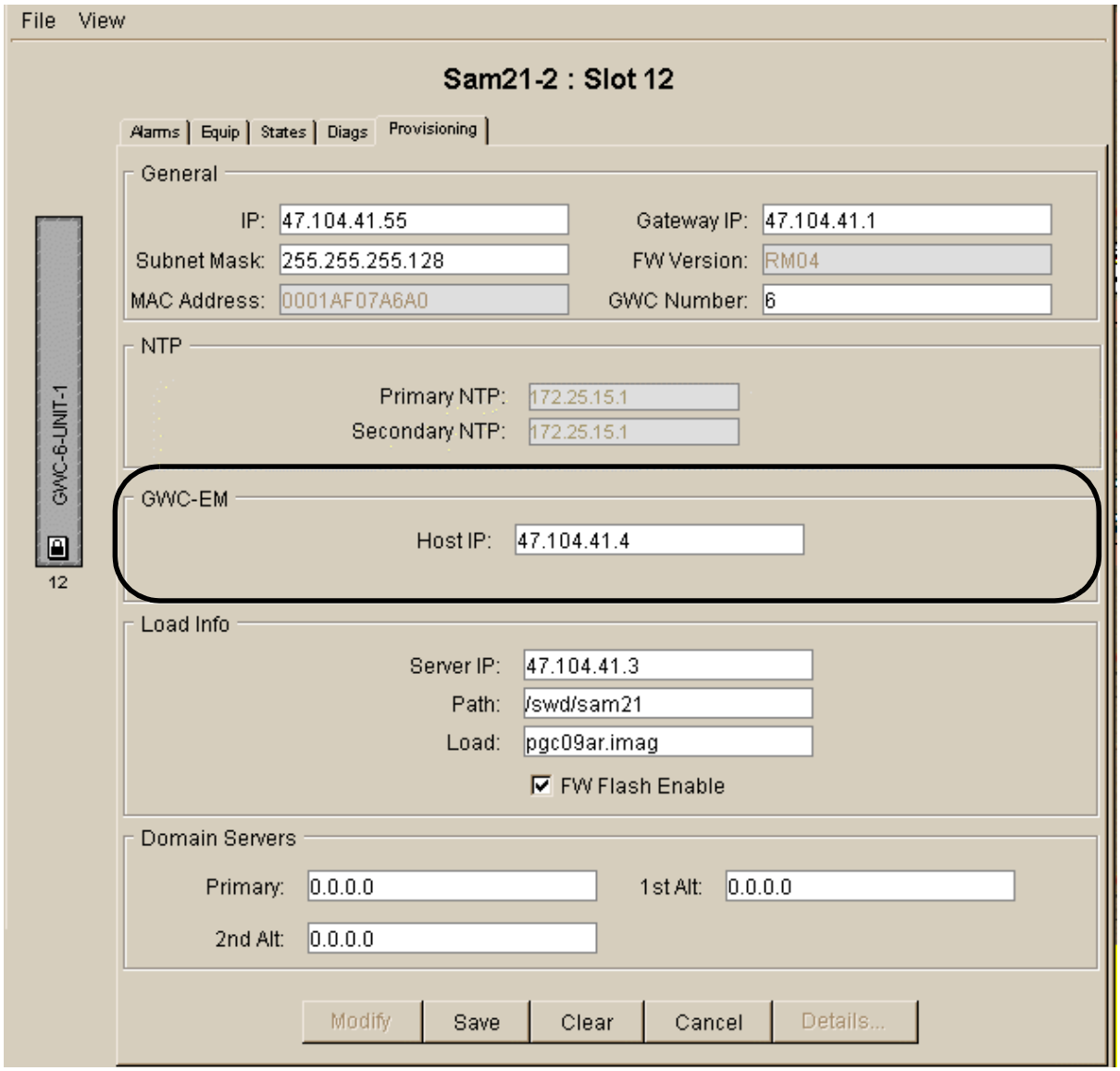
1 If an RTS failure occurs on the inactive GWC unit and the active GWC unit is not “Unlocked” and “Enabled”, then wait for it to become so. If it does not become “Unlocked” and “Enabled”, then lock the active GWC unit from the CS 2000 SAM21 Manager. Locking the Active GWC unit will force a SwAct to the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

If the RTS fails after a warm SwAct, go to the troubleshooting procedure Warm SwAct failed on page 179.

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 180.



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



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

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

Warm SwAct failed

At the CS 2000 SAM21 Manager client

1 From the CS 2000 SAM21 Manager verify that the inactive unit has properly loaded and RTS'd. If not, retry loading the GWC using troubleshooting procedure GWC does not RTS on page 176.

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.

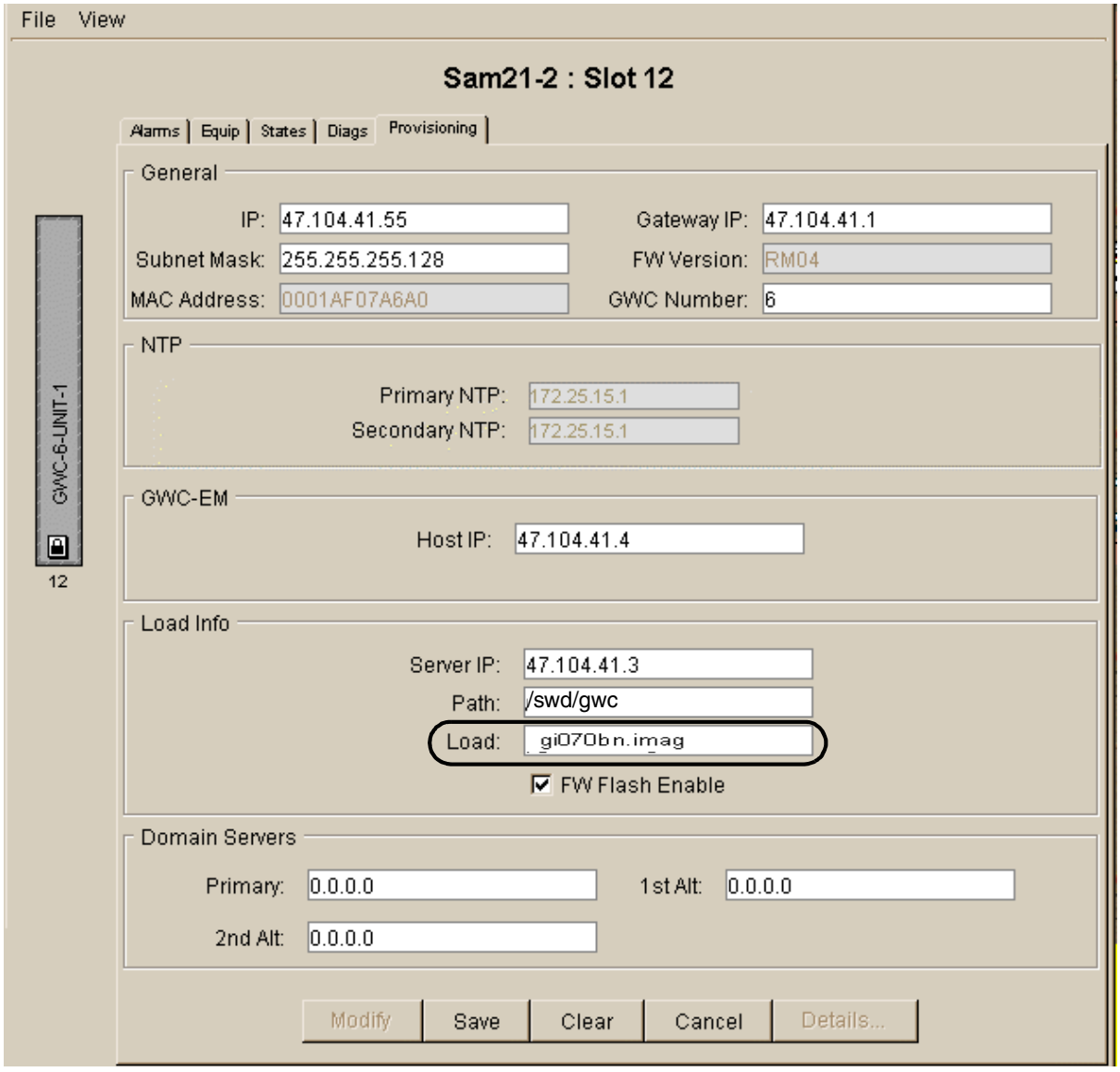
At the CS 2000 SAM21 Manager client

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.



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 183.

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.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Upgrade a GWC node's hardware - MCPN750 to MCPN905

Purpose of this procedure

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

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

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

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

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

When to use this procedure

This procedure is optional. However, in SN09 the following new profiles are available for use with MCPN905 GWC cards:

- higher density small line gateway profile
- higher density large line gateway profile
- combination line, trunk and audio controller profile

This upgrade procedure must be completed on both cards before one of the new profiles can be applied. The MCPN905 GWC card provides greater BHHCA capacity for trunk profiles. Nortel also recommends upgrading to the MCPN905 card for GWCs using an H.323 profile.

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

Prerequisites

CAUTION

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

The prerequisites for this procedure are as follows:

- The GWC must be operating as a duplex node (that is, one MCPN750 running as the active unit, and another MCPN750 as the warm standby unit).
- The upgrade requires two MCPN905 cards.
- The SAM21 EM and SAM21 Shelf Controller must be already upgraded.
- The GWC EM must be already upgraded.

Action

At the SAM21 chassis

1 BSY the Inactive unit.

2 Lock the Busy unit.

3 Unprovision the locked unit.

4 Remove the unprovisioned MCPN750 blade.

5 Insert an MCPN905 blade.

6 Provision the blade as a GWC.

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

7 Unlock the locked MCPN905.

8 RTS the MCPN905.

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

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

11 BSY the Inactive unit (MCPN750).

12 Lock the BUSY unit.

13 Unprovision the locked unit.

14 Remove the unprovisioned MCPN750 blade.

15 Insert an MCPN905 blade.

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

16 Provision the blade as a GWC.

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

17 Unlock the locked MCPN905.

18 RTS the inactive MCPN905.

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

20 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Confirming Gateway Controller loads after an upgrade

Use this procedure to confirm each Gateway Controller has the correct software load after an upgrade. Repeat this procedure for each Gateway Controller with upgraded software.

Prerequisites

Perform this procedure after you complete the upgrade of software on a Gateway Controller.

Action

Confirming SAM21 Shelf Controller loads after an upgrade

From the Application Launch Point

1 Launch the CS 2000 Management Tools application. If prompted, enter your Login Name and Password.

Response

The main CS 2000 Management Tools window appears.

2 Under Device Types, select Gateway Controller.

Response

Network-level information on Gateway Controllers appears.

3 Under Gateway Controllers, select an upgraded Gateway Controller.

Response

The Maintenance tab for the selected Gateway Controller appears.

4 Check the value in Loadname for each unit. Make sure the load name identifies the new load for the upgraded Gateway Controller.

5 Use the following table to determine your next step.

If the load names for both units	Do
identify the new load	step 6
anything else	Troubleshoot the problem or contact your next level of support. The upgrade was unsuccessful.

6 Use the following table to determine your next step.

If you	Do
need to check additional Gateway Controllers	step 3
completed checking all upgraded Gateway Controllers	step 8

7 Exit the CS 2000 Management Tools application.

8 You have completed this procedure