APPENDIX A

Performing GSS Software Upgrades and Downgrades

This appendix describes how to upgrade the GSS software to a new software version. To upgrade the software, you must do the following:

- Have access to the GSS download area of the Cisco software download site on Cisco.com.
- Be familiar with the proper procedure for updating your GSS devices and know the CLI commands required to execute the backup.

To take full advantage of all of the features and capabilities of the software release, we recommend that you upgrade all GSS devices in your network within the same time frame, starting with the primary GSSM. This upgrade sequence ensures that the other GSS devices properly receive configuration information from, and are able to send statistics to, the primary GSSM.

The GSS software upgrade requires that you comply with the software upgrade prerequisites and complete each of the procedures in the order shown in this appendix.

This appendix contains the following major sections:

Cisco-Supported Hardware and Software Compatibility

Note The GSS software release 4.1(0) is supported *only* on GSS 4492R, and is not supported on the following hardware: GSS 4491, GSS 4490, or GSS 4480.

When installed on a GSS 4492R, GSS 4491, GSS 4490, or GSS 4480, GSS software version 3.1(0) operates with all load balancers if ICMP, TCP, or HTTP-HEAD-type keepalives are used. In addition, you can use KAL-AP-type keepalives with the following Cisco products to support more effective load balancing:

- Cisco Content Services Switch (CSS)
- Cisco Catalyst 6500 Series Content Switching Module (CSM)
- Cisco Application Control Engine (ACE) module and appliance

Caution The GSS model 4480 cannot support all of the version 3.1(0) software functionality when it is operating as the primary GSSM; therefore, you cannot use this combination of hardware and software platforms as a primary or standby GSSM. Because the GSS 4480 is approaching its end-of-life target date, you must contact your Cisco representative regarding a hardware upgrade.

GSS software version 3.1(0) operates with the following Cisco hardware:

- CSS running the following WebNS software releases:

Cisco CSS Platform	Recommended WebNS Versions	Minimum Supported WebNS Versions
Cisco 11500 Series CSS	Software releases: • 7.40.0.04 or greater • 7.30.2.03 or greater	Software releases: • 7.20.1.04 • 7.10.3.05
Cisco 11000 Series CSS	Software releases: • 6.10.4.05 or greater • 5.00.6.05 or greater	Software releases: • 6.10.1.07 • 5.00.3.09

- Catalyst 6500 Series CSM running the following software releases:

Platform	Recommended CSM Versions[1]	Minimum Supported CSM Versions
Catalyst 6500 Series	Software releases: • 3.1(10) or greater • 3.2(1) • 4.1(4) or greater • 4.2(1) or greater	Software releases: • 3.1(4) • 3.2(1) • 4.1(4) • 4.2(1)

1. CSM software versions 3.2(2), 3.2(3), and 4.1(2) are not supported by the GSS when using the KAL-AP by tag keepalive method.

- ACE module or appliance running the following software releases:

Platform	Recommended ACE Versions	Minimum Supported ACE Versions
Cisco ACE 4700 Series Appliances	Software releases: • 3.0(0)A3(1.0) or greater	Software releases: • A1(8.0a)
Cisco ACE Modules	• 3.0(0)A2(1.0) or greater	• 3.0(0)A2(1.0)

In addition, you can use scripted keepalives with the following Cisco and non-Cisco hardware.

Device	Scripted Keepalive Types	Platform	Recommended Software Version
CSS	CSS wrapper	Cisco 11500 series CSS	SLB: 7.40.0.04 or greater
	SNMP_mib_not_index_by_vip	Cisco 11000/11500 series CSS	SLB: 6.10.4.05 or greater for 11000 series
	Snmp-scalar		SLB: 7.40.0.04 or greater for the 11500 series
CSM	CSM wrapper	Cisco Catalyst 6500 CSM	IOS: 12.2
	SNMP_mib_not_index_by_vip		CSM: 4.2(1)
	Snmp-scalar		

Note: Non-Cisco SLBs are supported for scripted keepalives. For more information, see Chapter 5, Configuring Keepalives, in the *Cisco Global Site Selector CLI-Based Global Server Load- Balancing Configuration Guide*.

Understanding the Software Upgrade Sequence for v4.1(0)

When upgrading your GSS devices to software version 4.1(0), you must complete the applicable upgrade sequence on each GSS device in the network. You must also complete an upgrade before you change the role of a GSS device (see the "Verifying the GSSM Role in the GSS Network" section). This section contains the following topic:

Upgrade Sequence for v4.1(0)

Table A-1 provides information about the upgrade sequence for previous software versions before you upgrade to version 4.1(0).

Table A-1 GSS Software Upgrade Sequence for 4.1(0)

From version . . .	To version . . .
1.0(x) or 1.1 (prior to 1.1.(1.7.0))	1.1.(1.7.0)
1.1.(1.7.0)	1.2.(2.2.0)
1.2 (x) where x = 1 or 2	1.3(3)
1.3(3)	4.1(0)

Table A-1 GSS Software Upgrade Sequence for 4.1(0)

From version . . .	To version . . .
2.0(1)	4.1(0)
2.0(2)	
2.0(3)	
2.0(4)	
2.0(5)	
3.0(1)	
3.0(2)	
3.1(0)	
3.1(1)	
3.1(2)	
3.2(0)	

Note When upgrading the GSS device from software versions that earlier than 3.2(0) to software Version 4.1(0), the device will reboot twice to complete the upgrade.

Beginning with version 1.3(x), alternate sequential paths might exist that provide a more direct path to the targeted upgrade version. For example, to upgrade from version 2.0(1) to version 3.1(0), you can use the following sequential upgrade path:

2.0(1) > 2.0(2) > 2.0(3) > 2.0(4) > 3.0(1) > 3.0(2) > 3.1(0) > 4.1(0)

You also can use the more direct path as follows:

2.0(1) > 4.1(0)

Note The GSS software release 4.1.0 is supported *only* on GSS 4492R, and is not supported on the following hardware: GSS 4491, GSS 4490, or GSS 4480.

Note You must upgrade the primary GSSM first, followed by the other GSS devices in your network. After you upgrade the primary GSSM, ensure that each GSS device in your network to be upgraded is connected to the primary GSS device. If you upgrade the non-primary GSS prior to the primary GSSM upgrade, you might experience unexpected behavior.

Verifying the GSSM Role in the GSS Network

Before you begin the upgrade procedure, verify that the roles of the designated primary and standby GSSMs have not changed. The changing of roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM is back online.

To verify the role of the current primary GSSM and the standby GSSM, perform the following steps:

1. At the CLI of the current primary GSSM, enter the following commands:

```
gssm1.example.com# cd /home
gssm1.example.com# type ../props.cfg | grep -i fqdn
```

The following output appears:

```
controllerFqdn= domain_name or ip_address
```

2. Based on the output value for controllerFqdn, follow these guidelines:

- If the value of the domain name or IP address is the current primary GSSM in your network, then the current primary GSSM and standby GSSM configuration is the original configuration and no further action is needed.
- If the value of the domain name or IP address is the current standby GSSM in your network, then the current primary GSSM and standby GSSM configuration is not the original configuration. In this case, you must reverse the roles of the primary and standby GSSM devices to those of the original GSS network deployment. See the "Reversing the Roles of the Interim Primary and Standby GSSM Devices" section in Chapter 2, Managing the GSS from the CLI.
- If the value of the domain name or IP address is not the current primary GSSM or the standby GSSM in your network, this indicates that the device is not a primary GSSM or is no longer on the network.

Obtaining a Software Upgrade File

Note You must have a Cisco.com username and password to download a software update from Cisco.com. To acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link.

You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number to obtain a Cisco.com username and password.

To obtain an upgrade file for the GSS software, perform the following steps:

1. Launch your preferred web browser and point it to the Cisco Global Site Selector download page. When prompted, log in to Cisco.com using your designated Cisco.com username and password. The Cisco GSS Software download page appears, listing the available software upgrades for the GSS software product.

   If you do not have a shortcut to the Cisco Global Site Selector download page, perform the following steps:

   a. Log in to Cisco.com using your designated Cisco.com username and password.
   b. Access the Software Center from the Technical Support link.
   c. Click the **Content Networking Software** link from the Software Center - Software Products and Downloads page.
   d. Click the **Cisco Global Site Selector** link from the Software Center - Content Networking page.
   e. Click the **Download Cisco Global Site Selector** link from the Software Center - Content Networking page.

   The Cisco GSS Software download page appears, listing the available software upgrades for the Cisco GSS Software product.

Note When you first access the Content Networking page of the Software Center, you must apply for eligibility for GSS software updates because it is considered a strong encryption image. Under the Cisco Content Networking Cryptographic Software section is the Apply for 3DES Cisco Cryptographic Software Under Export Licensing Controls link. Click this link and complete the Encryption Software Export Distribution Authorization Form. Complete this step to access and download Global Site Selector software images.

2. Locate the .upg file that you want to download by referring to the Release column for the proper release version of the software.
3. Click the link for the .upg file. The download page appears.
4. Click the **Software License Agreement** link. A new browser window opens to display the license agreement.
5. After you have read the license agreement, close the browser window that displays the agreement and return to the Software Download page.
6. Click **Download**. If prompted by the software, reenter your username and password.
7. Click **Save to file** and then choose a location on your workstation to temporarily store the .upg upgrade file.
8. Post the .upg file that you downloaded to a designated area on your network that is accessible to all of your GSS devices using FTP or SCP.

You are now ready to upgrade the software on a GSS device. See the "Preparing the GSS for a Software Upgrade" section.

Preparing the GSS for a Software Upgrade

Before upgrading a GSS to version 4.1(0), perform the following software upgrade prerequisites:

- Back up your current primary GSSM database—Before you upgrade, you must back up your current primary GSSM database in the event that you need to restore your database (see the "Performing a Full Primary GSSM Backup" section in Chapter 7, Backing Up and Restoring the GSSM Database). The GSSM database maintains all network and device configuration information and the DNS rules that are used by your GSS devices to route DNS queries from users to available hosts.

  If necessary, you can quickly restore your GSS network to its previous state by performing a full backup at any time. A full backup does not interfere with the functions of the primary GSSM or other GSS devices.

  If you have CNR loaded on the primary GSSM, you must disable CNR before you back up your current primary GSSM database and then enable CNR when you complete the upgrade (see the "Preparing the GSS for a Software Upgrade when CNR is Loaded" section).

- Ensure that you are running one of the following software versions: 2.0(3), 2.0(4), 2.0(5), 3.0(1), or 3.0(2), 3.1.(0)—If your GSS devices are not currently running one of the specified versions, then you must first upgrade to one of them before performing the version 4.1(0) upgrade (see the Understanding the Software Upgrade Sequence for v4.1(0) section).

Caution When a primary GSSM has been upgraded to version 3.3(0), but other GSS devices remain at or below version 2.0(4), global server load-balancing configuration settings do not propagate to the GSS devices at or below version 2.0(4). To avoid this behavior, ensure that all GSS devices on the network are upgraded to the same software version as the primary GSSM before you configure global server load balancing.

Preparing the GSS for a Software Upgrade when CNR is Loaded

In addition to the software upgrade prerequisites described in the "Preparing the GSS for a Software Upgrade" section, you must perform the following action items when you have CNR loaded and enabled on the GSS:

- To obtain support for reverse lookup for the answers configured on the GSS, you need to explicitly configure the Pointer (PTR) records to do the same on CNR (see the CNR documentation on cisco.com).
- To perform NS forwarding on GSS version 3.1(0) without CNR to a name service that is a GSS with CNR, you must configure a proper domain name in the domain name field in the NS type answer configuration. In addition, the external name server must be authoritative for the domain name if the name server is a GSS with CNR. By default, the NS type answer queries for ".". See the *Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide* for information about configuring NS forwarding.
- To obtain the same expiration level for the records returned by the GSS and the CNR, you need to ensure that the TTL configuration is the same on both the CNR (see the CNR documentation on cisco.com) and GSS (see the *Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide)*.
- To have the GSS/CNR device process the NON A records for the authoritative domain, you must configure all the NON A records on the CNR that were earlier processed by the external name service using NS forwarding (see the CNR documentation on cisco.com for more information).

Note Prior to the release of GSS software version 3.1, Cisco announced the end-of-sale and end-of-life dates for an option to run Cisco Network Registrar within the GSS, thus enabling the GSS to have full DNS server capabilities. As a result of this announcement, new SF-GSS-DNSLIC software licenses that enable the integrated CNR are no longer available. To request more information regarding this change, including guidance for migration options from the integrated version of CNR running on the GSS, send your request to ask-gss@cisco.com.

Performing a Software Upgrade

Before installing a new software image, ensure that you have reviewed and comply with the software upgrade prerequisites described in the "Preparing the GSS for a Software Upgrade" and "Preparing the GSS for a Software Upgrade when CNR is Loaded" sections.

Note When upgrading the GSS device from software versions that are lower than 3.3(0) to software version 4.1(0), the device reboots twice before the upgrade procedure is complete.

Note Be sure to upgrade the primary GSSM first, followed by the other GSS devices in your network. After you upgrade the primary GSSM, ensure that each GSS device in your network to be upgraded has connectivity to the primary GSSM before you perform the software upgrade procedure on them.

Note Upgrading your GSS devices causes a temporary loss of service for each affected device.

To upgrade the GSS software (starting with the primary GSSM), perform the following steps:

1. Log on to the CLI of the GSS device.
2. Enter the Global Configuration Mode by entering the **enable** command and then the **config** command.
3. If you use FTP to copy files into GSS, enable the FTP client by entering the **ftp-client enable all** command at the config prompt.
4. Type **exit** to leave Global Configuration mode.
5. Use the **ftp** or **scp** command to copy the GSS software upgrade file from the network location to a directory on the GSS. Ensure that you set the transfer type to **binary**.

   For example, to copy an upgrade file named gss.upg from a remote host, your FTP session may appear as follows:

```
gssm1.example.com# ftp host.example.com
Connected to host.example.com.
220 host.example.com FTP server (Version wu-2.6.1-0.6x.21) ready.
Name (host.example.com:root): admin
331 Password required for admin.
Password:
230 User admin logged in. Access restrictions apply.
Remote system type is UNIX.
Using ascii mode to transfer files.
ftp> binary
ftp> get
(remote-file) gss.upg
(local-file) gss.upg
local: gss.upg remote: gss.upg
200 PORT command successful.
```

6. Enable privileged EXEC mode.

```
gssm1.example.com> enable
gssm1.example.com#
```

7. Stop the GSS software by entering the following command:

```
gssm1.example.com# gss stop
```

8. If the GSS has CNR loaded on it, enter the Global Configuration Mode by entering the **enable** command and then the **config** command.

   If the GSS does not have CNR loaded on it, skip ahead to Step 11.

9. Disable CNR if the GSS has CNR loaded on it.

```
gssm1.example.com (config)# no cnr enable
```

10. Type **exit** to leave Global Configuration mode.
11. Install the upgrade by entering the following command:

```
gssm1.example.com# install gss.upg
```

This command performs a validation check on the upgrade file, unpacks the upgrade archive, and installs the software upgrade.

12. At the Proceed with install (the device will reboot)? (y/n): prompt, enter **y** to reboot the GSS device. After the GSS reboots, you lose any network CLI connections. Console connections remain active.

Note If you did not previously save changes to the startup-config file, the Save current configuration? [y/n]: prompt appears. At the prompt, enter **y** to continue. The GSS then reboots.

13. After the GSS device reboots, log in to the GSS device and enable privileged EXEC mode.
14. Verify that the GSS device reaches a normal operation state of runmode 4 or 5 by entering the **gss status** command.
15. Enter configuration mode and enable CNR if the GSS has CNR loaded on it.

```
gssm1.example.com# config
gssm1.example.com (config)# cnr enable
```

16. Repeat the entire procedure for the remaining GSS devices in your network.

Downgrading Software Versions on GSS Devices

Observe the following hardware platform-dependent rules when downgrading your GSS devices to a software version lower than version 3.1(0):

- Model 4492 platform—Supports software downgrades to version 1.3(2) or higher only. This model does not support the versions lower than version 1.3(2) because of a change to the OS kernel.
- Model 4491 platform—Supports software downgrades to version 1.2(2) or higher only. This model does not support the versions lower than version 1.2(2) because of a change to the OS kernel.
- Model 4490 platform—Supports software downgrades to version 1.2(2) or higher only. This model does not support the versions lower than version 1.2(2) because of a change to the OS kernel.
- Model 4480 platform—Supports all software downgrade versions. To downgrade the software on a 4480 device to a version lower than version 1.3(2), you must make RMA arrangements to return the devices to Cisco for the downgrade.

Note If the GSS has CNR loaded on it, the lowest software version that you can downgrade to is version 2.0(1); however, we recommend that you do not downgrade lower than GSS version 2.0(3) when using CNR.

Caution A version 3.x database cannot run on the earlier software platforms because of changes in the database schema and kernel. For this reason, we do not recommend that you downgrade to a lower version from version 3.x with the current GSLB configuration. After the downgrade, you must restore the backup of the primary GSSM database that corresponds to the downgrade software version. For example, if you want to downgrade to version 2.0(3), you must have a software release version 2.0(3) database backup that you can restore.

To perform a downgrade, you must disable the entire GSS network.

If you have any questions about the need to downgrade your system, contact Cisco Technical Assistance Center (TAC). See the "Obtaining Documentation and Submitting a Service Request" section for more information.

This section contains the following topics:

Downgrading to Version 1.3(2) or Higher

Use the procedure in this section to downgrade to software version 1.3(2) or higher on any of the four GSS models. If you are downgrading a 4491 or 4490 to a version lower than version 1.3(2), see the "Downgrading a GSS 4490 or GSS 4491 to Version 1.3 (1) or Lower" section.

Note If you use CNR with your GSS devices, the lowest software version that you can downgrade the GSS mesh to is version 2.0(1); however, we recommend that you do not downgrade lower than GSS version 2.0(3) when using CNR.

To downgrade to version 1.3(2) or higher, perform the following steps:

1. Obtain a copy of the downgrade software version (see the "Obtaining a Software Upgrade File" section).
2. Ensure that you have a copy of the database that was saved when the version of software that you are downgrading to was running on the GSS.
3. Disable the GSS network by performing the following steps on each GSS:
   a. Stop the GSS software by using the **gss stop** command in privileged EXEC mode.

      ```
      gssm1.example.com# gss stop
      ```

   b. If CNR is loaded on any of the GSS devices, enter configuration mode and disable CNR by using the **no cnr enable** command.

      ```
      gssm1.example.com (config)# no cnr enable
      ```

      If CNR is not loaded on the GSS, skip ahead to Step d.

   c. Type **exit** to exit configuration mode.
   d. Disable the GSS by using the **gss disable** command in privileged EXEC mode.

      ```
      gssm1.example.com# gss disable
      ```

4. Install the downgrade by using the **install** command in privileged EXEC mode.

   ```
   gssm1.example.com# install gss.upg
   ```

   This command performs a validation check on the upgrade file, unpacks the upgrade archive, and installs the software upgrade.
5. At the Proceed with install (the device will reboot)? (y/n): prompt, enter **y** to reboot the GSS device. After the GSS reboots, you lose any network CLI connections. Console connections remain active.

Note If you did not previously save changes to the startup-config file, the Save current configuration? [y/n]: prompt appears. At the prompt, enter **n** to continue. The GSS then reboots.

6. After the GSS device reboots, log in to the GSS device and enable privileged EXEC mode.
7. Verify that the GSS device reaches a normal operation state of runmode 4 or 5 by using the **gss status** command in privileged EXEC mode.
8. Restore the database (see Chapter 7, "Backing Up and Restoring the GSSM Database").
9. Enable CNR if the GSS has CNR loaded on it by using the **cnr enable** command in configuration mode.

   ```
   gssm1.example.com (config)# cnr enable
   ```

10. Repeat Steps 3 through 9 for the remaining GSS devices in your network.

Downgrading a GSS 4490 or GSS 4491 to Version 1.3 (1) or Lower

Use the procedures in this section to downgrade a GSS 4491 or GSS 4490 to a version of software that is version 1.3(1) or lower, with the lowest supported version being version 1.2(2). For all other types of GSS downgrades, see the "Downgrading to Version 1.3(2) or Higher" section.

Note If the GSS has CNR loaded on it, the lowest software version that you can downgrade to is version 2.0(1); however, we recommend that you do not downgrade lower than GSS version 2.0(3) when using CNR.

The requirements to downgrade a GSS 4491 or GSS 4490 to a version of software that is version 1.3(1) or lower are as follows:

- Full backup of your primary GSSM database—You need the database backup that corresponds to the software version to which you want to restore. Use the backup to restore the database on the primary GSSM after the downgrade.
- Recovery image and associated recovery CD—You obtain a recovery image for the specific downgrade version from Cisco and then create a CD from the image.
- Keyboard, mouse, and monitor—You must connect locally to the GSS to perform the types of software downgrades described in this section.

This section contains the following topics:

Obtaining a Recovery Image and Creating a Recovery CD

This section describes how to obtain the recovery image from Cisco and create a recovery CD. If necessary, contact Cisco Technical Assistance Center (TAC) for more information about obtaining the recovery image.

You must have a Cisco.com username and password to download a software update from Cisco.com. To acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link. You also need a service contract number, Cisco.com registration number and verification key, Partner Initiated customer Access (PICA) registration number and verification key, or packaged service registration number to obtain a Cisco.com username and password.

To obtain the recovery image and create a CD, perform the following steps:

1. Use your preferred web browser to access the recovery image at https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=GSS_Forum
2. Locate the GSSRecoverySoftware.iso file. Confirm these file properties:
   - owner: rongole
   - date: 16-MAY-2006
   - size: 194117632 bytes
3. Click on the file. If prompted by the software, reenter your username and password, and then click **OK**.

Note The GSS recovery software is considered a strong encryption image. If you are not eligible to receive strong encryption images, you will be prompted to complete the Encryption Software Distribution Authorization Form. Complete the form to access and download the GSS recovery software.

4. If prompted, complete the Encryption Software Distribution Authorization Form (see the previous Note).
5. When the End User License Agreement opens, read the license agreement, and then click **I agree**. The File Download page opens.
6. Click **Save**, and then choose a location on your workstation to temporarily store the recovery file.
7. Use your preferred CD-creation software to burn the recovery file to a CD.
8. Before attempting to use the recovery CD, run an md5 checksum on the file using a tool, such as md5sum on Linux, and confirm that the value is b84ff87e04f7b2a95dcf2afe06b02f01.

Downgrading GSS 4490 Devices to Version 1.3(1) or Lower

Before you downgrade, perform the following steps:

1. Verify the role of the primary GSSM in the GSS network (see the "Verifying the GSSM Role in the GSS Network" section).
2. Connect your keyboard and mouse to their corresponding ports on the GSS 4490 device.
3. Connect the monitor to the GSS console port.

To use the recovery CD to downgrade each GSS 4490 device on your network, perform the following steps:

1. Insert the recovery CD into the CD-ROM drive on the GSS.
2. Power cycle the GSS and press **F1** during the initial startup sequence to enter the BIOS Setup.
3. Choose **Start Options**, and then press **Enter**.
4. Choose **Startup Sequence**, and then press **Enter**.
5. Navigate to First Startup Device, and then change the state to **Disabled**.
6. Navigate to Second Startup Device, and then change the state to **Disabled**.
7. Navigate to First Startup Device again, and then choose **CD-ROM**.
8. Navigate to Second Startup Device again, and then choose **Hard Disk 0**.

9. Press **Esc** three times. When prompted, choose **If yes, Save and Exit the Setup Utility**, and then press **Enter**. The GSS boots from the recovery CD and displays the Rescue prompt.
10. Enter **gss-rescue** at the prompt, and then press **Enter**.
11. When "Sleeping..." displays, press the **Ctrl**, **Alt**, and **Delete** keys or power cycle by pressing the power button to reboot the GSS, and then press **F1** during the initial startup sequence to reenter the BIOS Setup.
12. Power cycle the GSS and press **F1** during the initial startup sequence to enter the BIOS Setup.
13. Choose **Start Options**, and then press **Enter**.
14. Press **Enter** again to select Startup Sequence.
15. Navigate to First Startup Device, and then change the state to **Disabled**.
16. Navigate to Second Startup Device, and then change the state to **Disabled**.
17. Navigate to First Startup Device again, and then choose **Hard Disk 0**.
18. Navigate to Second Startup Device again, and then choose **CD-ROM**.
19. Press **Esc** three times. When prompted, choose **If yes, Save and Exit the Setup Utility**, and then press **Enter**. The GSS boots.
20. Restore your primary GSSM (see the "Restoring a Primary GSSM Backup" section in Chapter 7, Backing Up and Restoring the GSSM Database).

Downgrading GSS 4491 Devices to Version 1.3(1) or Lower

Before you downgrade, perform the following steps:

1. Verify the role of the primary GSSM in the GSS network (see the "Verifying the GSSM Role in the GSS Network" section).
2. Connect your keyboard and mouse to their corresponding ports on the GSS 4491 device.
3. Connect the monitor to the GSS console port.

To use the recovery CD to downgrade each GSS 4491 device on your network, perform the following steps:

1. Insert the recovery CD into the CD-ROM drive on the GSS.
2. Power cycle the GSS and press **F4** during the initial startup sequence to enter the BIOS Setup.
3. At the BIOS Setup screen, choose the **Boot menu**.
4. Choose the **Boot Device Priority** menu.
5. Choose **ATAPI CD-ROM** as the first device from which to boot.
6. Save the settings and exit from the BIOS. The GSS boots from the recovery CD and displays the Rescue prompt.
7. Enter **gss-rescue** at the prompt, and then press **Enter**.
8. When "Sleeping..." displays, press the **Ctrl**, **Alt**, and **Delete** keys or power cycle by pressing the power button to reboot the GSS, and then press **F4** during the initial startup sequence to reenter the BIOS Setup.
9. At the BIOS Setup screen, choose the **Boot** menu, choose the **Boot Device Priority menu**, and then choose **Hard Drive** as the first device from which to boot.
10. Save the settings.
11. Remove the recovery CD and then exit from the BIOS. The GSS boots.

12. Restore your primary GSSM (see the "Restoring a Primary GSSM Backup" section in Chapter 7, Backing Up and Restoring the GSSM Database).