CHAPTER 2

Managing the GSS from the CLI

This chapter describes how to manage the GSS software from the CLI. It contains the following major sections:

Logging in to the CLI and Enabling Privileged EXEC Mode

To log in to a GSS device and enable privileged EXEC mode at the CLI, perform the following steps:

1. Press the power control button on the GSS. After the GSS boot process completes, the software prompts you to log in to the device.
2. If you are remotely logging in to the GSS device (Global Site Selector or Global Site Selector Manager) through Telnet or SSH, enter the hostname or IP address of the GSS to access the CLI.

   Otherwise, if you are using a direct serial connection between your terminal and the GSS device, use a terminal emulation program to access the GSS CLI.

Note For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

3. Specify your GSS administrative username and password to log in to the GSS device. The CLI prompt appears.

   ```
   localhost.localdomain>
   ```

4. At the CLI prompt, enable privileged EXEC mode.

   ```
   localhost.localdomain> enable
   localhost.localdomain#
   ```

   The prompt changes from the user-level EXEC right angle bracket (>) prompt to the privileged-level EXEC pound sign (#).

Understanding GSS Software Licenses

A license package is a predefined set of features bundled together and sold as an upgrade to the GSS v1.3 software. You can view a GSS software license as a collection of license packages. For the v2.0 release, GSS capabilities have been extended through a product coupling with the Cisco Network Registrar (CNR). In addition, GSS now includes support for Distributed Denial of Service (DDoS) attack detection and mitigation.

The CNR and DDoS licenses are add-ons; you must separately purchase and install these two licenses. For a detailed overview and description of the CNR and DDoS features, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide.*

To install either the CNR or DDoS license, your GSS must be running software version 2.0(2) or higher. All previous version features are available and configurable immediately except for the specifically licensed features. If you want to enable the DDoS license package on a particular GSS, you must purchase a DDoS license from Cisco Systems in order to receive a Product Access Key (PAK) number.

Ensure that each GSS in your GSS network possesses a unique license file to avoid any potential problems. Do *not* install the same licence file (files with the same PAK number) in more than one GSS in the network. If you use the same PAK number, the GSS with the duplicate license file will be deregistered from the GSS network. If a clash of duplicate PAK numbers occurs between the primary GSSM and any other GSS in the network, the other GSS is de-registered even if you installed a valid PAK number on it prior to installing a PAK number on the primary GSSM.

To recover a deregistered GSS, perform the following steps:

1. Uninstall the duplicate license file by using the **license uninstall** command.
2. Stop and then disable the GSS as described in the "Stopping the GSS Software" and "Disabling the GSS Software" sections.
3. Reregister the GSS as the primary GSSM. See Chapter 1, Managing GSS Devices from the GUI, for more details.

This section contains the following topics:

Acquiring and Installing CNR and DDoS License Files

The Software Infrastructure and Fulfillment Technology (SWIFT) application is a web-based package provided by Cisco that:

- Allows you to retrieve or generate a license file for a particular PAK.
- Provides a way for Cisco to track licenses as well as a way for you to recover lost licenses.
- Enables internal support organizations to obtain information about customer licenses.

To obtain a license file, perform the following steps:

1. Connect to the Cisco SWIFT web site at the following URLs.
   - Use the following website if you are a registered user of Cisco Connection Online:

     https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
   - Use the following website if you are not a registered user of Cisco Connection Online:

     https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

   You will be prompted for various details about your purchase as part of a software registration process.
2. Enter the required data. After submitting this data, the web site authenticates the information, generates a license file, and emails it to you.

Note We recommend that you make a back-up copy of your license file after you receive it by email in case the license file is lost or corrupted. Should anything happen to your license file, SWIFT also enables you to regenerate it.

3. Transfer the license file from your PC to the GSS using FTP.

   For example, transfer a license file to the GSS as follows:

```
C:\>ftp 1.1.1.21
Connected to 1.1.1.21.
220 "Global Site Selector FTP"
User (1.1.1.21:(none)): admin
331 Please specify the password.
Password:*****
230 Login successful.
ftp> bin
200 Switching to Binary mode.
ftp> put cnr_new.lic
200 PORT command successful. Consider using PASV.
150 Ok to send data.

226 File receive OK.
ftp: 696 bytes sent in 0.00Seconds 696000.00Kbytes/sec.
ftp> quit
221 Goodbye.
```

4. Install the license once you have transfered your license file by using the **license** command. A valid license file always includes the .lic extension. Otherwise, it is considered invalid and is not installed.

   For example, you can install a DDoS license as follows:

```
gssm1.example.com# license install ddos_new.lic
```

   The license file is copied to the /licenses directory when the installation is complete.

5. To uninstall a license file on the GSS, enter the **license** command with the **uninstall** keyword as follows:

```
gssm1.example.com# license uninstall ddos_new.lic
```

Installing CNR

To install CNR, you must first obtain the following:

- GSS license, SF-GSS-DNSLIC
- CNR software, CNR-6.3-BASE1K (CNR software 6.3 or higher)
- CNR license file/key, shipped with the CNR software

Note Your GSS network must be running software version 2.0(2) or higher.

To install CNR on the GSS, perform the following steps:

1. Specify the license for the CNR module on the GSS as show in the following example:

   ```
   gssm1.example.com# license install GSS20070920122230075.lic
   ```

   To verify the proper installation of the GSS and CNR license, enter the **show license** command as follows:

   ```
   gssm1.example.com# show license installed

   License modules are
   CNR
   ```

2. Install the CNR software on the GSS.

   a. Enable the GSS to serve as an FTP client.

   ```
   gssm1.example.com# config t
   gssm1.example.com (config)# ftp-client enable admin
   gssm1.example.com (config)# exit
   ```

   b. From the GSS CLI, download the CNR software from the FTP server. The software is automatically placed in the default FTP directory.

   ```
   gssm1.example.com# ftp 1.1.1.23
   Connected to 1.1.1.23 (1.1.1.23).
   220 3Com 3CDaemon FTP Server Version 2.0
   Name (1.1.1.23): cisco
   331 User name ok, need password
   Password:
   230 User logged in
   Remote system type is UNIX.
   Using binary mode to transfer files.
   ```

```
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get cnr_6_2_3-linux.gtar.gz
local: cnr_6_2_3-linux.gtar.gz  remote: cnr_6_2_3-linux.gtar.gz
227 Entering passive mode ...
125 Using existing data connection
##################.....
226 Closing data connection; File transfer successful.
31625689 bytes received in 0.0013 secs (2.4e+02 Kbytes/sec)
ftp> quit
221 Service closing control connection
gssm1.example.com#
```

c. Install the CNR software on the GSS by using the **cnr install** command and specifying the CNR license key as shown in the following example:

```
gssm1.example.com# cnr install cnr_6_3-linux.gtar.gz
cnr-license xxxx-xxxx-xxxx-xxxx
Installing CNR from cli-install. This may take a few minutes.
```

If you provide an invalid or expired license key, an error message appears and the installation halts. The installation will then remove the CNR installation directory, which may result in the removal of any previous versions or installations of CNR.

Note The CNR installation does not activate the CNR server agent. You must explictly enable CNR to start processing requests. See Step 4.

3. Verify that the GSS software is running:

```
gssm1.example.com# gss status

Cisco GSS - 2.0(2) GSSM - primary [Thu Nov  8 14:27:33 EDT 2007]

Normal Operation [runmode = 5]

 START  SERVER
 Oct25  Boomerang
     ?  CNR DNS Server              [ Server is not ready ]
     ?  CNR Server Agent            [ Server is not ready ]
 Oct25  Config Agent (crdirector)
 Oct25  Config Server (crm)
 Oct25  DNS Server
 Oct25  Database
 Oct25  GUI Server (tomcat)
 Oct25  Keepalive Engine
```

```
 Oct25  Node Manager
 Oct25  Proximity
 Oct25  Sticky
 Oct25  Web Server (apache)
 Oct25  drp
```

If necessary, enable the GSS software. For example, to configure the selected device to act as the primary GSSM for your GSS network, enter the following command:

```
gssm1.example.com# gss enable gssm-primary
```

See the *Cisco Global Site Selector Getting Started Guide* for details.

4. Enable the CNR server agent by using the **cnr enable** command in global configuration mode as shown in the following example:

```
gssm1.example.com# config
gssm1.example.com (config)# cnr enable
# Starting Network Registrar Local Server Agent
```

If you did not properly install CNR on the GSS, the **cnr enable** command displays a message informing you to first install the CNR license.

```
gssm1.example.com (config)# cnr enable
CNR enable failed. Please install CNR first
```

5. Verify that the CNR license installed properly:

```
gssm1.example.com# show license gss-all
Own (Primary GSS) info:
Pak number is:
DDOS Not Installed, Not Active
CNS Installed, Active
```

6. Verify that the CNR software is running on the primary GSSM:

```
gssm1.example.com# gss status

Cisco GSS - 2.0(2) GSSM - primary [Thu Nov  8 14:31:28 EDT 2007]

Normal Operation [runmode = 5]

 START  SERVER
 14:28  Boomerang
 14:30  CNR DNS Server
 14:30  CNR Server Agent
 14:28  Config Agent (crdirector)
 14:28  Config Server (crm)
```

```
14:28  DNS Server
14:28  Database
14:28  GUI Server (tomcat)
14:28  Keepalive Engine
14:27  Node Manager
14:28  Proximity
14:28  Sticky
14:28  Web Server (apache)
14:28  drp
```

Accessing the CNR CLI

The CNR command-line interface (the **nrcmd** program) allows you to control your local cluster servers' operations by setting all configurable options, as well as starting and stopping the servers.

To access the **nrcmd** program, perform the following steps:

1. Enter the **cnr** command in the GSS privileged EXEC mode.

   ```
   gssm1.example.com# cnr
   ```

   You must install and enable CNR on the GSS before you can enter the CNR **nrcmd** program. Otherwise, an error message appears.

2. Enter the username and password when the prompts appear.

   ```
   username: <user_name>
   password: ******
   100 OK
   session:
       cluster = localhost
       current-vpn = global
       default-format = user
       groups = superuser
       roles = superuser
       scope-edit-mode = staged
       user-name = admin
       visibility = 5
       zone-edit-mode = synchronous
   nrcmd>
   ```

   See the *Cisco CNS Network Registrar CLI Reference Guide, 6.3* for instructions on using **nrcmd**.

3. Exit the CNR **nrcmd** program.

```
nrcmd> exit
gssm1.example.com#
```

Invoking the Shell and Executing CNR Utilities

The GSS provides a restricted CNR shell that supports built-in Linux commands, such as **cd** and **echo**. It also supports numerous CNR utilities including:

- **cnr_tactool**—Packages CNR data for TAC support engineers for troubleshooting purpose.
- **cnr_exim**—Exports or imports CNR data repositories.
- **cnr_keygen**—Generates keys for Secret Key Transaction Authentication for DNS (TSIG) configuration or key import.

To invoke the CNR shell and execute the CNR utilities, perform the following steps:

1. Enter the **cnr shell** command in the GSS privileged EXEC mode.

   ```
   gssm1.example.com# cnr shell
   ```

2. Press the **Tab** key in the CNR shell to display the supported utilities.

   ```
   cnr shell> cnr <Tab>
   cnr_exim        cnr_tactool.orig  cnrdb_load     cnrdb_verify
   cnr_exim.orig   cnrdb_archive     cnrdb_printlog cnrservagt
   cnr_keygen      cnrdb_checkpoint  cnrdb_recover  cnrsnmp
   cnr_keygen.orig cnrdb_deadlock    cnrdb_stat     cnr_tactool
   cnrdb_dump      cnrdb_upgrade     cnr shell >    cnr shell
   ```

3. Enter the utility name to execute any of these CNR utilities. For example:

   ```
   cnr shell> cnr_tactool
   user:
   password:
   ```

   See the *Cisco CNS Network Registrar User's Guide* for more information about **cnr_tactool** and the other available CNR utilities.

Using the startup-config and running-config Files

When you make device configuration changes, the GSS places those changes in a virtual running configuration file (called running-config). Before you log out or reboot the GSS, you must copy the contents of the running-config file to the startup-configuration file (called startup-config) to save configuration changes. The GSS uses the startup-config file on subsequent reboots.

This section contains the following procedures:

Changing the startup-config and running- config Files

The network configuration for a GSS device includes the following:

- Interface—Ethernet interface in use
- IP address—Network address and subnet mask assigned to the interface
- GSS communications—Interface (Ethernet 0 or Ethernet 1) designated for handling GSS-related communications on the device
- GSS TCP keepalives—Interface (Ethernet 0 or Ethernet 1) designated for outgoing keepalives of type TCP and HTTP HEAD
- Hostname—Hostname assigned to the GSS
- IP default gateway—Network gateway used by the device
- IP name server—Network DNS server being used by the device
- IP routes—All static IP routes
- SSH enable—SSH state of the GSS device (enabled or disabled)
- Telnet enable—Telnet state of the GSS device (enabled or disabled)
- FTP enable—FTP state of the GSS device (enabled or disabled)
- FTP client enable—FTP client state of the GSS device (enabled or disabled)

- SNMP enable—SNMP state of the GSS device (enabled or disabled)

Each GSS device tracks the following configurations:

- Startup configuration—Default network configuration. The GSS loads the startup configuration settings each time you boot the device.
- Running configuration—Network configuration currently in use by the GSS device.

Typically, the running-config and the startup-config files are identical. Once you modify a configuration parameter, you must reconcile the two configuration files in one of the following ways:

- Save the running-config file as the new startup-config file by using the **copy running-config startup-config** command. The GSS retains any changes to the network configuration of the device and uses those changes when the GSS is next rebooted.
- Maintain the startup-config file. In this case, the GSS device uses the running-config file until you reboot the device. The GSS then discards the running-config file and restores the startup-config file.

To change the startup-config file for a GSS device, perform the following steps:

1. Log in to the CLI, enable privileged EXEC mode, and access global configuration mode on the device.

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

2. Make any desired changes to the GSS configuration. For example, to change the device hostname, use the **hostname** command in global configuration mode as follows:

```
gssm1.example.com(config)# hostname new.example.com
new.example.com(config)#
```

3. Copy the current running-config file as the new startup-config file for the GSS by entering the following command:

```
new.example.com(config)# copy running-config startup-config
```

Saving the startup-config and running-config Files

To save the running-config file to the startup-config file on the GSS, or to copy the current startup configuration to a file for use on other devices or for backup purposes, use one of the following commands:

- **copy startup-config disk** *filename*—Copies the GSS device startup configuration to a named file on the GSS.
- **copy running-config disk** *filename*—Copies the GSS device current running configuration to a named file on the GSS.
- **copy running-config startup-config**—Copies the GSS device current running configuration as the new startup configuration.

To copy the GSS device running-config or startup-config files, perform the following steps:

1. Log in to the CLI of the primary GSSM, standby GSSM, or a GSS device and enable privileged EXEC mode.

   ```
   gss1.example.com> enable
   gss1.example.com#
   ```

2. Copy the current startup configuration to a file for use on other devices or for backup purposes by entering the following command:

   ```
   gss1.example.com# copy startup-config disk newstartupconfig
   ```

   The *filename* argument specifies the name of the file containing the startup configuration settings.

Note The primary GSSM backup does not include user files that reside in the /home directory. If you want to have a secure copy of the GSS startup-config file, use either the secure copy (**scp**) or **ftp** commands to copy the startup-config file to another device. Storing the startup-config file in a safe location can save time and reconfiguration issues in a recovery situation.

3. Copy the GSS device current running configuration to a named file located on the GSS by entering the following command:

   ```
   gss1.example.com# copy running-config newrunningconfig
   ```

The *filename* argument specifies the name of the file containing the running configuration settings.

4. Save the running-config file as the new startup-config file by entering the following command:

```
gss1.example.com# copy running-config startup-config
```

The GSS retains any changes to the network configuration of the device and uses those changes when the GSS is next rebooted.

Loading the startup-config from an External File

In addition to copying your running-config file as a new startup-config file, you can also upload or download GSS device configuration information from an external file using the **copy** command. Before you attempt to load the startup configuration from a file, make sure that the file has been moved to a local directory on the GSS device.

To load the GSS device startup configuration from an external file, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

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

2. Load the GSS device startup configuration settings from a named file located on the GSS by entering the following command:

```
gssm1.example.com# copy disk startup-config newstartupconfig
```

The *filename* argument specifies the name of the file containing the startup configuration settings.

Displaying the running-config File

You can review the contents of the GSS running-config file to verify the current configuration parameters in use by the GSS device. To display the contents of the GSS running-config file, use the **show running-config** command. You can use this command with the **show startup-config** command to compare the configuration memory to the startup-config file used during the bootup process.

Configuration entries within each mode in the running-config file appear in chronological order, based on the order in which you configure the GSS. The GSS does not display default configurations in the running-config file.

To display the current running-config file for the GSS, enter the following command:

```
gssm1.example.com# show running-config
interface ethernet 0
   ip address 192.168.1.25 255.255.255.0
   gss-communications
   gss-tcp-keepalives

hostname gssm1.example.com
ip default-gateway 10.86.208.1
ip name-server 172.16.124.122

ssh enable
no ssh keys
no ssh protocol version 1
telnet enable
ftp enable
ftp-client enable all
ntp enable
snmp enable
snmp community-string
    <set>
ntp-server 16.1.1.11
cnr enable
drp
    enable
    authentication key sample key
    path-rttprobe
        burst_size 5
        init_ttl 2
        destination-port 1020
        max-failure-ttl 5
        max-ttl 40
    tcp-rttprobe
        sourceport static 10

terminal length 23
exec-timeout 150

logging disk enable
logging disk priority Notifications(5)
no logging host enable
logging host priority Warnings(4)
```

```
tacacs-server timeout 5
tacacs-server keepalive-enable
```

Displaying the startup-config File

You can review the contents of the GSS startup-config file to display the configuration used during initial bootup. The GSS stores the contents of the startup-config file in a safe partition of the hard disk to prevent loss of data due to power failures.

To display the contents of the GSS startup-config file, enter the following command:

```
gssm1.example.com# show startup-config
GSS configuration [Saved: Thu Jul 10 16:20:25 UTC 2003]

interface ethernet 0
   ip address 192.168.1.25 255.255.255.0
   gss-communications
   gss-tcp-keepalives

hostname gssm1.example.com
ip default-gateway 10.86.208.1
ip name-server 172.16.124.122
ssh enable
no ssh keys
no ssh protocol version 1
telnet enable
ftp enable
ftp-client enable all
ntp enable
snmp enable
snmp community-string
    <set>

ntp-server 16.1.1.11
cnr enable
```

```
drp
    enable
    authentication key sample key
    path-rttprobe
        burst_size 5
        init_ttl 2
        destination-port 1020
        max-failure-ttl 5
        max-ttl 40
    tcp-rttprobe
        sourceport static 10

terminal length 23
exec-timeout 150
logging disk enable
logging disk priority Notifications(5)
no logging host enable
logging host priority Warnings(4)

tacacs-server timeout 5
tacacs-server keepalive-enable
```

Managing GSS Files

This section describes how to manage the files included in a directory or subdirectory on a GSS device. This section contains the following topics:

Displaying the Contents of a File

You can view the contents of a GSS file and monitor functions such as transaction logging or system logging using the system.log file. Use the **tail** and **type** CLI commands to view the contents of a file in a GSS directory as follows:

- Display the last 10 lines of a file within any GSS file director by using the **tail** *filename* command. This command displays the end of a file within any GSS file directory.
- Display the entire contents of a file within any GSS file directory by using the **type** *filename* command.

The *filenam*e argument identifies the name of the file in the GSS file directory. To view the files available in the current directory or subdirectory, use the **dir**, **lls**, **ls**, or **pwd** commands. See the "Displaying Files in a Directory" section for details.

For example, to display the last 10 lines in the system.log, enter:

```
gssm1.example.com# tail system.log
Showing file system.log
Sep 15 07:11:40 host-css2 rc: Stopping keytable succeeded
Sep 15 07:11:42 host-css2 inet: inetd shutdown succeeded
Sep 15 07:11:45 host-css2 crond: crond shutdown succeeded
Sep 15 07:11:46 host-css2 dd: 1+0 records in
Sep 15 07:11:46 host-css2 dd: 1+0 records out
Sep 15 07:11:46 host-css2 random: Saving random seed succeeded
Sep 15 07:11:48 host-css2 kernel: Kernel logging (proc) stopped.
Sep 15 07:11:48 host-css2 kernel: Kernel log daemon terminating.
Sep 15 07:11:50 host-css2 syslog: klogd shutdown succeeded
Sep 15 07:11:51 host-css2 exiting on signal 15
End of file system.log
```

For example, to display the contents of the audit.log file, enter:

```
gssm1.example.com# type /audit.log
atcr1.cisco.com>type audit.log

# Start logging at Tue July 1 23:59:30 GMT 2003
#=== WHEN                        WHAT_TABLE     WHAT_ID          HOW
===

# Start logging at Wed July 2 00:01:25 GMT 2003
#=== WHEN                        WHAT_TABLE     WHAT_ID          HOW
===

# Start logging at Thu July 3 14:42:40 GMT 2003
#=== WHEN                        WHAT_TABLE     WHAT_ID          HOW
===
...
```

Displaying Files in a Directory

The GSS software directories contain the GSS files, including boot files, backup files, and log files. Use the **dir**, **lls**, **ls**, or **pwd** commands to view the files available in the current directory or subdirectory on the GSS as follows:

- **dir** [*directory*]—Displays a detailed list of files contained within the working directory on the GSS, including names, sizes, and time created. You may optionally specify the name of the directory to list. The equivalent command is **lls**.
- **lls** [*directory*]—Displays a detailed list of files contained within the working directory on the GSS, including names, sizes, and time created. You may optionally specify the name of the directory to list. The equivalent command is **dir**.
- **ls** [*directory*]—Displays a detailed list of filenames and subdirectories within the working directory on the GSS, including filenames and subdirectories. You may optionally specify the name of the directory to list.
- **pwd** - Displays the current working directory of the GSS.

To view a detailed list of files contained within the working directory, enter:

```
gssm1.example.com# dir     (or lls)
total 97684
-rw-r--r--    1 root     root           39 Mar  8 21:04 JVM_EXIT_CODE
-rw-r--r--    1 root     root            9 Mar 14 21:23 RUNMODE
-rw-r--r--    1 root     root        33427 Mar 14 21:23 gss.log
drwxr-xr-x    2 root     root         4096 Mar  7 16:22 admin
drwxr-xr-x    3 root     root         4096 Mar  7 18:05 apache
-rw-r--r--    1 root     root          117 Mar  7 18:05 audit.log
srwxr-xr-x    1 root     root            0 Mar  7 15:40 cli_config
srwxr-xr-x    1 root     root            0 Mar  7 15:40 cli_exec
drwxr-xr-x   14 root     root         4096 Mar  7 18:05 core-files
-rw-r--r--    1 root     root           61 Mar 14 21:23 datafeed.cfg
srwxrwxrwx    1 root     root            0 Mar  7 15:40
dataserver-socket
-rw-r--r--    1 root     root           18 Mar  7 15:39 nicinfo.cfg
-rw-r--r--    1 root     root         5072 Mar  7 18:05 node.state
drwxrwxrwx    2 root     root         4096 Mar  8 21:04 pid
-rw-rw-rw-    1 root     root         9127 Mar 14 21:23 props.cfg
-rw-r--r--    1 root     root           63 Mar 14 21:23
runmode-comment
-rw-r--r--    1 root     root          553 Mar  8 21:02 running.cfg
drwxr-xr-x    4 root     root         4096 Mar  8 18:34 squid
```

```
-rw-r--r--    1 root     root           49 Mar  7 18:05
sysMessages.log
drwxr-xr-x    2 root     root         4096 Mar  7 15:40 sysmsg
drwxrwxrwx    2 root     root         4096 Mar  8 21:02 sysout
-rw-r--r--    1 root     root        41652 Mar 14 21:23 system.log
```

To list the filenames and subdirectories of the current working directory, enter:

```
gssm1.example.com# ls
gss-1.0.2.0.2-k9.upg    id_rsa.pub        megara.back.1_0.full  rpms
gss-1.0.904.0.1-k9.upg  gss_sample.full   megara.back.1_1.full
```

To display the present working directory of the GSS, enter:

```
gssm1.example.com# pwd
/admin
```

Renaming GSS Files

The GSS software allows you to rename files located in the current directory or subdirectory, such as backup files and log files. To rename a GSS file, use the **rename** command. The syntax for this command is as follows:

rename *source_filename new_filename*

The arguments are:

- *source_filename*—Alphanumeric name of the file that you want to rename.
- *new_filename*—Alphanumeric name to assign to the file.

Quotation marks are not required around filenames. The following special characters are not allowed in the renamed filenames: apostrophe (‘), semicolon (;), asterisk (*), and space ( ).

To view the files available in the current directory or subdirectory, use the **dir**, **lls**, **ls**, or **pwd** commands. See the “Displaying Files in a Directory” section for details.

For example, to rename the current GSS startup-config file as *newstartupconfig*, enter:

```
gssm1.example.com# rename startup-config newstartupconfig
```

Securely Copying Files

The GSS supports the secure copying of files from the GSS device where you are logged in, or from another device to the GSS device where you are currently logged in.

Note The GSS supports one-way communication only in SCP. You can copy GSS files from the GSS where you are logged in to an external device. You can also copy files from an external device to the GSS. However, from an external device, you cannot execute the **scp** command and get files from the GSS. You can only use **scp** from the GSS.

Use the **scp** command to securely copy files from the following:

- A GSS device that you are logged in to:

  scp {*source_path* [*source_filename*] *user@target_host***:***target_path*}

- Another device to the GSS device that you are currently logged in to:

  scp {*user@source_host***:/***source_path*[*source_filename*] *target_path*}

The argument are as follows:

- *source_path*—Relative directory path and filename on the source device of the file being transferred.
- *source_filename*—Name of the file to be copied.
- *user@target_host*—Login account name and hostname for the device to which you are copying files.
- *target_path*—Relative directory path on the target device to which the file is being copied.
- *user@source_host*— Login account name and hostname for the device from which you are copying files.

After you log in to the CLI of the GSS that you intend to copy files to or from, enter the **scp** command as previously described. You may be prompted to log in to the remote device before you can navigate to the target directory.

To securely copy files from a GSS device that you are logged in to, enter:

```
gssm1.example.com# scp /tmp/system.log
myusername@192.168.2.3:/dump/home
```

To securely copy files from another device to a GSS device that you are currently logged in to, enter:

```
gssm1.example.com# scp <file-name of the GSS>
username@remote-host:target-path
```

Deleting Files

The GSS allows you to remove a specific file (startup-config, logs, or archive file) stored on hard disk. You may want to remove older files or files that you no longer use from the GSS. To delete files from your GSS, use the **del** command.

The syntax for this command is as follows:

del *filename*

The *filenam*e argument identifies the name of the file in the GSS file directory.

For example, to delete the *oldtechrept.tgz file*, enter:

```
gssm1.example.com# del oldtechrept.tgz
```

Displaying Users

You can display the username and permission status for a specific user or for all users of the GSS device as follows:

- Use the **show user** *username* command to display user information for a particular user. The *username* argument identifies the name of the GSS user that you want to display information for.
- Use the **show users** command to display information for all GSS users.

To display information for a particular user, enter:

```
gssm1.example.com#show user paulr-admin
Username     permission
--------     ----------
paulr-admin  admin
```

To display information for all users, enter:

```
gssm1.example.com# show users
Username     permission
--------     ----------
```

```
lstar         admin
admin         admin
paulr-admin   admin
```

For details about creating GSS users, refer to Chapter 3, Creating and Managing User Accounts.

Specifying the GSS Inactivity Timeout

You can modify the length of time that can expire before a GSS automatically logs off an inactive user by using the **exec-timeout** command. This command specifies the length of time that a user in privileged EXEC mode can be idle before the GSS terminates the session. Users logged on to GSS devices in the global configuration mode are not affected by the **exec-timeout** command setting. The default inactivity timeout value is 150 minutes.

The syntax for the **exec-timeout** command is as follows:

exec-timeout *minutes*

The *minutes* argument specifies the length of time that a user in privileged EXEC mode can be idle before the GSS terminates the session. Valid entries are 1 to 44,640 minutes. The default is 150 minutes.

For example, to specify a GSS timeout period of 10 minutes, enter:

```
gssm1.example.com(config)# exec-timeout 10
```

To restore the default timeout value of 150 minutes, use the **no** form of this command.

Configuring the Terminal Screen Line Length

You can specify the number of screen lines to display on your terminal by using the **terminal length** command. The maximum number of displayed screen lines is 512. The default is 23 screen lines. When the **terminal length** command is set to a value of 0, the GSS sends all of its data to the screen at once without pausing to buffer the data. To restore the default terminal length of 23 lines, use the **no** form of this command.

The syntax for this command is as follows:

terminal-length *number*

The *number* argument specifies the number of screen lines to display on your terminal, from 0 and 512. The default is 23 lines.

For example, to set the number of screen lines to 35, enter:

```
gssm1.example.com(config)# terminal-length 35
```

To reset the number of screen lines to the default of 23, enter:

```
gssm1.example.com(config)# no terminal-length
```

To display the terminal length setting for your GSS device, use the **show terminal-length** command.

For example:

```
gssm1.example.com# show terminal-length
terminal length 35
```

Modifying the Attributes of the Security Certificate on the GSSM

You can customize the attributes of the security certificate issued by Cisco Systems and installed on the primary GSSM (as described in the "Logging Into the Primary GSSM Graphical User Interface" section in Chapter 1, , Managing GSS Devices from the GUI). By using the **certificate set-attributes** CLI command, you can modify the X.509 fields, extensions, and properties included on the security certificate. The attribute changes that you make affect the fields on the Details tab of the certificate. To return the attributes for the security certificate to the default settings, use the **no** form of the **certificate set-attributes** command.

When you enter the **certificate set-attributes** command, the GSS software displays a series of prompts related to the fields on the certificate. Proceed though all of the prompts and make changes only to those fields that you want to modify. When completed, the software prompts you to save your changes and generate a a new certificate. The next time that you access the primary GSSM GUI, the Security Alert dialog box reappears informing you that the certificate is invalid. At that point, you can either reinstall the updated certificate or close the dialog box and continue with the primary GSSM GUI operation.

To modify the attributes of a security certificate on the primary GSSM, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

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

2. Enter the **gss stop** command to stop the GSS software. Modifications to the certificate cannot occur while the GUI is active on the primary GSSM.

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

3. Access global configuration mode on the device.

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

4. Enter the **certificate set-attributes** command and modify information at the prompts. All fields displayed for each software prompt have a maximum character limit of 64, except for Country Code, which has a maximum character limit of 2.

```
gssm1.example.com(config)# certificate set-attributes
Country code (2 chars) [US]:
State [California]: MA
City [San Jose]: Boston
Organization [Cisco Systems, Inc.]: New Organization
Organization Unit [ISBU]:
e-Mail Address [tac@cisco.com]: company@mycompany.com

US
MA
Boston
New Organization
ISBU
company@mycompany.com
```

5. Enter **y** to save these values (or **n** to use the existing certificate values).

```
Save these values? (y/n): y
```

6. Restart the GSS device.

```
gssm1.example.com(config)# exit
gssm1.example.com# gss start
```

Stopping the GSS Software

You must stop the GSS software before you perform the following tasks:

- Upgrade GSS software
- Perform a warm reboot
- Restore GSS factory defaults
- Disable an active GSS device
- Perform GSS maintenance or troubleshooting

Use the **gss stop** command to stop the GSS software. For example, enter:

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

The following message appears when you stop the GSS software from the CLI.

```
Server is Shutting Down
```

Use the **gss start** command to restart the GSS software on the selected device after it has been stopped. For example, enter:

```
gssm1.example.com# gss start
```

Shutting Down the GSS Software

If you intend to power down a GSS device, we recommend that you use the **shutdown** command to first shut down the GSS software. You should also shut down the GSS software before you disable a GSS (see the "Disabling the GSS Software" section).

To shut down the GSS software, enter:

```
gssm1.example.com# shutdown
```

Restarting the GSS Software

You can perform a warm restart of the GSS software by using the **gss restart** command. Before you perform a warm restart of the GSS software, save your recent GSS configuration changes to memory. Use the **copy running-config startup-config** CLI command to save your configuration changes. If you fail to save your configuration changes, the GSS device reverts to its previous settings upon a reboot.

To perform a warm restart of the GSS, enter:

```
gssm1.example.com# gss restart
```

As the GSS reboots, the output appears on the console terminal.

Performing a Cold Restart of a GSS Device

You can halt GSS operation and perform a cold restart of your GSS device by using the **reload** command. The **reload** command reboots the GSS device and performs a full power cycle of both the GSS hardware and software. Any open connections with the GSS are dropped after you enter the **reload** command.

Before you perform a cold restart of the GSS, save your recent GSS configuration changes to memory. Use the **copy running-config startup-config** CLI command to save your configuration changes. If you fail to save your configuration changes, the GSS device reverts to its previous settings upon restart.

To halt and perform a cold restart of the GSS, enter:

```
gssm1.example.com# reload
```

As the GSS boots, the output appears on the console terminal.

Disabling the GSS Software

Disabling a GSS device is necessary when you need to perform the following tasks:

- Switch the role of a GSS within a network
- Change a GSS to a GSSM

- Move a GSS or GSSM to a different network of GSS devices

Use the **gss disable** command to disable a selected GSSM or GSS. This command removes the existing configuration and returns the GSS device to its initial state, which includes deleting the GSSM database from the GSS device and removing all configured DNS rules and keepalives. The **gss disable** command also removes any certificate attributes specified using the **certificate set-attributes** command.

To disable a GSS device, enter:

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

To reenable the GSS device as a primary GSSM, standby GSSM, or a GSS, see the *Cisco Global Site Selector Getting Started Guide*.

Restoring GSS Factory-Default Settings

The **restore-factory-defaults** command erases your GSSM database and all of its data and resets all network settings, returning your GSS hardware to the same state it was in when it first arrived from the factory. If your GSS device is improperly configured, use the **restore-factory-defaults** command to restore the device to its initial state and allow you to properly configure the GSS device for use on your network.

Before you enter the **restore-factory-defaults** command, ensure that you back up any vital data in the database component of the primary GSSM, along with its network and device configuration information. Use the **gssm backup** command to perform a primary GSSM backup. See Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database for details.

Caution User files will also be deleted when you enter the **restore-factory-defaults** command. If you have any important files in the /home directory that you want to save, use either the secure copy (**scp**) or **ftp** commands to copy those files before you enter the **restore-factory-defaults** command.

Enter the **gss stop** command before you execute the **restore-factory-defaults** command to stop the GSS software and avoid disrupting in-process activities (for example, serving DNS requests or sending keepalives).

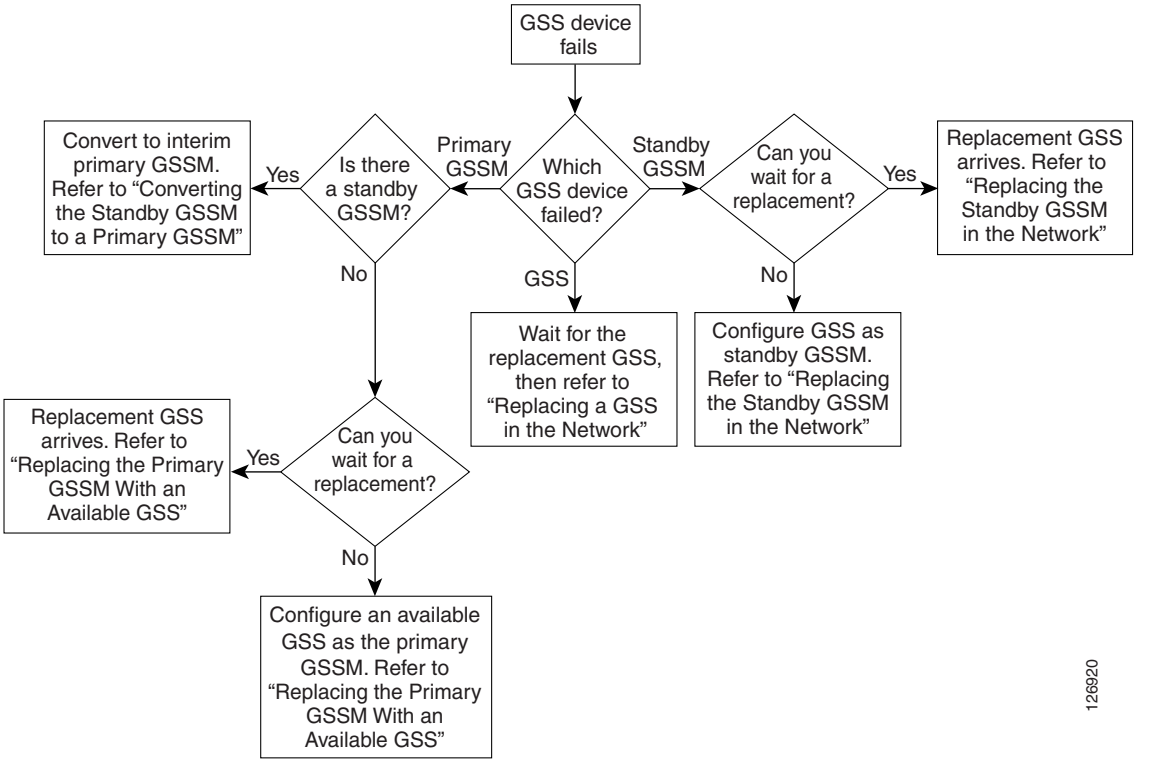
To restore GSS factory default settings, enter:

```
gssm1.example.com# gss stop
gssm1.example.com# restore-factory-defaults
```

Replacing GSS Devices in Your GSS Network

If you encounter problems with one of the GSS devices in your network, determine which GSS device contains the problem (primary GSSM, standby GSSM, or GSS) and configure a replacement GSS device for your network. Figure 2-1 summarizes the decision-making process to follow when replacing a malfunctioning GSS device.

Figure 2-1 Flow Chart for Replacing a Malfunctioning GSS Device



This section contains the following topics:

Replacing the Primary GSSM in the Network

To replace a malfunctioning primary GSSM in your GSS network to regain GUI management, determine if there is a standby GSSM available in your network:

- If you have a standby GSSM that you can convert to the primary GSSM, see the "Converting the Standby GSSM to a Primary GSSM" section.
- If you do not have a standby GSSM but do have an available GSS that you can convert to the primary GSSM, see the "Replacing the Primary GSSM with an Available GSS" section.

Converting the Standby GSSM to a Primary GSSM

Note Ensure that the designated primary GSSM is either offline or configured as a standby GSSM before you attempt to enable the standby GSSM as the new interim primary GSSM. Having two primary GSSM devices active at the same time may result in the inadvertent loss of configuration changes for your GSS network.

To convert the standby GSSM to a primary GSSM, perform the following steps:

1. Log in to the CLI of the primary GSSM, enable privileged EXEC mode, and perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the "Performing a Full Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database).
2. Log in to the CLI of the standby GSSM and enable privileged EXEC mode.

```
gssm2.example.com> enable
gssm2.example.com#
```

3. Configure the current standby GSSM to function as the temporary primary GSSM for your GSS network. Use the **gssm standby-to-primary** command to reconfigure your standby GSSM as the primary GSSM in your GSS network.

```
gssm2.example.com# gssm standby-to-primary
```

Note After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

4. Validate the database records of the interim primary GSSM by entering the following command.

```
gssm2.example.com# gssm database validate
```

5. Exit privileged EXEC mode. The standby GSSM begins to function in its new role as the interim primary GSSM and is now fully functional. You may now access the GUI.

6. When the replacement for the original primary GSSM is available, place the current interim primary GSSM in standby mode by entering the following command:

```
gssm2.example.com# gssm primary-to-standby
```

This command allows the current interim primary GSSM to resume its role in the GSS network as the standby GSSM.

7. Exit from the CLI of the standby GSSM.

8. Log in to the CLI of the GSS replacement for the original primary GSSM and enable privileged EXEC mode.

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

9. Configure basic network connectivity settings following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS. Specify the same hostname and IP address of the original primary GSSM.

10. Save your configuration changes to memory by entering the following command:

```
gssm1.example.com# copy running-config startup-config
```

11. Configure the GSS device as the replacement primary GSSM in the GSS network by entering the following command:

```
gssm1.example.com# gss enable gssm-primary
```

Note After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

12. Determine if you have a full backup of the interim primary GSSM database that you can restore on the new primary GSSM as follows:

- If yes, restore the interim primary GSSM database. See the "Restoring a Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database. You can now use the replacement primary GSSM in your GSS network.
- If no, determine if you have a backup of the original primary GSSM database as follows:
  - If yes, restore the original primary GSSM database. See the "Restoring a Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database. Verify the existing global server load-balancing configuration settings (DNS rules and keepalives) and modify the settings as described in the *Cisco Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version). You can now use the replacement primary GSSM in your GSS network.
  - If no, proceed to Step 13.

13. If you do not have a backup of either the interim or original primary GSSM database, do the following:

a. Reconfigure the global server load-balancing configuration settings on the new primary GSSM as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version).

b. Send DNS queries to the new primary GSSM and ensure that it replies properly to the queries. If the new primary GSSM replies properly, proceed to step 13c. If it fails to reply properly, verify the network connectivity settings and resend DNS queries to the device.

c. At the CLI of the standby GSSM and of each GSS device in your network, enter the **gss disable** command to remove the existing configuration, including the deletion of the GSSM database from the standby GSSM, and return the GSS device to an initial state. The deletion process includes removing all previously configured DNS rules and keepalives.

```
gssm2.example.com# gss disable
```

d. At the CLI of the standby GSSM, enter the **gss enable gssm-standby** command to configure the GSS device as the standby GSSM in the GSS network and direct it to the primary GSSM. See the "Replacing the Standby GSSM in the Network" section for details about the **gss enable gssm-standby** command.

```
gssm2.example.com# gss enable gssm-standby gssm1.example.com
```

e. At the CLI of each GSS, enter the **gss enable** command to enable your GSS device as a GSS and direct it to the primary GSSM. Specify either the domain name or the network address of the primary GSSM. See the "Replacing a GSS in the Network" section for details about the **gss enable** command.

Note You may want to perform this step on one GSS device at a time to minimize disruptions on your GSS network.

```
gss3.example.com# gss enable gss gssm1.example.com
```

f. Register the standby GSSM and each GSS device with the new primary GSSM. See the "Activating GSS Devices from the Primary GSSM" section in Chapter 1, , Managing GSS Devices from the GUI.

You can now use the replacement primary GSSM in your GSS network.

Replacing the Primary GSSM with an Available GSS

To replace a malfunctioning primary GSSM with an available GSS, perform the following steps:

1. Determine if you can wait for a replacement primary GSSM or if you require an immediate primary GSSM configuration change in your network to preserve the network configuration as follows:

- If yes, wait until the replacement GSS is available and configure it as the primary GSSM. Proceed to Step 6.
- If no, configure an available GSS device as the primary GSSM. Proceed to Step 2.

2. Log in to the CLI of the primary GSSM, enable privileged EXEC mode, and perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the "Performing a Full Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database.

3. Log in to the CLI of the GSS and enable privileged EXEC mode.

```
gss3.example.com> enable
gss3.example.com#
```

4. Stop the GSS software running on the GSS by entering the following command:

```
gss3.example.com# gss stop
```

5. Remove the existing configuration and return the GSS device to an initial state, including the removal of all previously configured DNS rules and keepalives, by entering the following command:

```
gss3.example.com# gss disable
```

6. If this is a new GSS device, configure basic network connectivity settings following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS. Ensure that you specify the same hostname and IP address of the original primary GSSM.

7. Save your configuration changes to memory by entering the following command:

```
gssm1.example.com# copy running-config startup-config
```

8. Configure the GSS device as the primary GSSM in the GSS network by entering the following command:

   ```
   gssm1.example.com# gss enable gssm-primary
   ```

9. Determine if you have a full backup of the original primary GSSM database that can be loaded on the replacement GSS as follows:

- If yes, restore the primary GSSM database as described in the "Restoring a Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database.
- If no, proceed to Step 10.

10. If you do not have a backup of the original primary GSSM database, do the following:

    a. Reconfigure the global server load-balancing configuration settings on the new primary GSSM as described in the *Cisco Global Site Selector Global Server Load-Balancing Configuration Guide* (GUI-based or CLI-based version).

    b. Send DNS queries to the new primary GSSM and ensure that it replies properly to the queries. If the new primary GSSM replies properly, proceed to Step 10c. If it fails to reply properly, verify the network connectivity settings and resend DNS queries to the device.

    c. At the CLI of the standby GSSM and of each GSS device in your network, enter the **gss disable** command to remove the existing configuration, including the deletion of the GSSM database from the standby GSSM, and return the GSS device to an initial state. The deletion process includes removing all previously configured DNS rules and keepalives.

       ```
       gssm2.example.com# gss disable
       ```

    d. At the CLI of the standby GSSM, enter the **gss enable gssm-standby** command to reenable the standby GSSM in the GSS network and direct it to the primary GSSM. See the "Replacing the Standby GSSM in the Network" section for details about the **gss enable gssm-standby** command.

       ```
       gss1.example.com# gss enable gssm-standby gssm1.example.com
       ```

e. At the CLI of each GSS, enter the **gss enable** command to enable your GSS device as a GSS and direct it to the primary GSSM. Specify either the domain name or the network address of the primary GSSM. See the "Replacing a GSS in the Network" section for details about the **gss enable** command.

Note You may want to perform this step on one GSS device at a time to minimize disruptions on your GSS network.

```
gss3.example.com# gss enable gss gssm1.example.com
```

f. Register the standby GSSM and each GSS device with the new primary GSSM. See the "Activating GSS Devices from the Primary GSSM" section in Chapter 1, Managing GSS Devices from the GUI.

You can now use the replacement primary GSSM in your GSS network.

Replacing the Standby GSSM in the Network

To replace a malfunctioning standby GSSM in your GSS network, perform the following steps:

1. Determine if you can wait for the replacement standby GSSM or if you require an immediate configuration change in your GSS network as follows:

- If yes, wait until the replacement GSS is available and configure it as the standby GSSM. Proceed to Step 5.
- If no, configure an available GSS device as the standby GSSM. Proceed to Step 2.

2. Log in to the CLI of the GSS and enable privileged EXEC mode.

```
gss3.example.com> enable
gss3.example.com#
```

3. Stop the GSS software running on the GSS by entering the following command:

```
gss3.example.com# gss stop
```

4. Disable the GSS to remove the existing configuration and return the GSS device to an initial state by entering the following command:

```
gss3.example.com# gss disable
```

This command removes all previously configured DNS rules and keepalives.

5. If this is a new GSS device, configure basic network connectivity following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
6. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

7. If this is an existing GSS device, delete it from your GSS network through the primary GSSM GUI. See the "Deleting GSS Devices" section in Chapter 1, , Managing GSS Devices from the GUI.
8. If you want to use the same hostname and IP address of the failed standby GSSM, determine if you have a backup of the startup-configuration file for that device as follows:

- If yes, reload the backup copy of the GSS device startup configuration settings (see the "Saving the startup-config and running-config Files" section).
- If no, reenter the platform configuration following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.

9. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

10. Configure the GSS device as the standby GSSM in the GSS network and direct it to the primary GSSM by entering the **gss enable gssm-standby** command.

    The syntax for this command is as follows:

    gss enable gssm-standby *primary_GSSM_hostname* | *primary_GSSM_IP_address*

    The argument are as follows:

    – *primary_GSSM_hostname*—DNS hostname of the device currently serving as the primary GSSM

– *primary_GSSM_IP_address*—DNS hostname of the device currently serving as the primary GSSM

For example, to enable gss3.example.com as the standby GSSM and direct it to the primary GSSM, gssm1.example.com, enter:

```
gss3.example.com# gss enable gssm-standby gssm1.example.com
```

11. Activate the standby GSSM from the primary GSSM GUI to add it to your GSS network. See the "Activating GSS Devices from the Primary GSSM" section in Chapter 1, , Managing GSS Devices from the GUI.

You can now use the replacement standby GSSM in your GSS network.

Replacing a GSS in the Network

To replace a malfunctioning GSS in your GSS network, perform the following steps:

1. Configure basic network connectivity for the replacement GSS device following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.
2. If you want to use the same hostname and IP address of the failed GSS, determine if you have a backup of the startup-configuration file for that device as follows:

- If yes, reload the backup copy of the GSS device startup configuration settings (see the "Saving the startup-config and running-config Files" section).
- If no, reenter the platform configuration following the procedures outlined in the *Cisco Global Site Selector Getting Started Guide*, Chapter 3, Setting Up Your GSS.

3. If this is an existing GSS device, delete it from your GSS network through the primary GSSM GUI. See the "Deleting GSS Devices" section in Chapter 1, , Managing GSS Devices from the GUI.
4. Enable your GSS device as a GSS and direct it to the primary GSSM in your GSS network by entering the **gss enable** command.

   The syntax for this command is:

   gss enable gss *primary_GSSM_hostname* | *primary_GSSM_IP_address*

The arguments are as follows:

- *primary_GSSM_hostname*—DNS hostname of the device currently serving as the primary GSSM.
- *primary_GSSM_IP_address*—DNS hostname of the device currently serving as the primary GSSM.

For example, to enable gss3.example.com as a GSS and direct it to the primary GSSM, gssm1.example.com, enter:

```
gss3.example.com# gss enable gss gssm1.example.com
```

5. Save your configuration changes to memory by entering the following command:

```
gss3.example.com# copy running-config startup-config
```

6. Activate the GSS from the primary GSSM GUI to add it to your GSS network. See the "Activating GSS Devices from the Primary GSSM" section in Chapter 1, , Managing GSS Devices from the GUI.

You can now use the replacement GSS in your GSS network.

Changing the GSSM Role in the GSS Network

The GSS software supports two GSSM devices in a single GSS network, with one GSSM acting as the primary GSSM and the second GSSM acting as a standby device. The standby GSSM can temporarily take over the role of the primary GSSM if the primary GSSM is unavailable (for example, you need to move the primary GSSM or you want to take it offline for repair or maintenance).

Using the CLI, you can manually switch the roles of your primary and standby GSSM devices at any time.

Before switching GSSM roles, follow these guidelines:

- You must configure and enable both a primary and a standby GSSM in your GSS network. Do not attempt to switch GSSM roles until you configure and enable both a primary and a standby GSSM (see the *Cisco Global Site Selector Getting Started Guide*).

- Ensure that the designated primary GSSM is either offline or configured as a standby GSSM before you attempt to enable the standby GSSM as the new primary GSSM. Having two primary GSSM devices active at the same time may result in the inadvertent loss of configuration changes for your GSS network.

  Although DNS request routing continues to function in such a situation, GUI configuration changes made on one or both primary GSSM devices may be lost or overwritten and are not communicated to the GSS devices. If this dual primary GSSM configuration occurs, the two primary GSSM devices change to standby mode. You must then reconfigure the original deployed primary GSSM as the primary GSSM.

- The switching 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. Use the interim primary GSSM to monitor GSS network behavior and, if necessary, to make configuration changes.

This section contains the following topics:

Switching the Roles of the Primary and Standby GSSM Devices

This procedure assumes that your primary GSSM is online and functional when you are switching GSSM roles. If the primary GSSM is not functional, proceed to Step 6.

To change the role of your primary and standby GSSM devices, perform the following steps:

1. Log in to the CLI and enable privileged EXEC mode.

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

2. Perform a full backup of your primary GSSM to preserve your current network and configuration settings (see the "Performing a Full Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database).

3. Configure the current primary GSSM as the standby GSSM. Use the **gssm primary-to-standby** command to place the primary GSSM in standby mode.

   ```
   gssm1.example.com# gssm primary-to-standby
   ```

4. (Optional) Power down the primary GSSM by entering the following command:

   ```
   gssm1.example.com# shutdown
   ```

5. Exit from the CLI of the primary GSSM.
6. Log in to the CLI of the standby GSSM and enable privileged EXEC mode.

   ```
   gssm2.example.com> enable
   ```

7. Configure the current standby GSSM to function as the temporary primary GSSM for your GSS network. Use the **gssm standby-to-primary** command to reconfigure your standby GSSM as the primary GSSM in your GSS network.

   ```
   gssm2.example.com# gssm standby-to-primary
   ```

Note After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

   Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

8. Validate the database records of the interim primary GSSM by entering the following command:

   ```
   gssm2.example.com# gssm database validate
   ```

9. Exit privileged EXEC mode. The standby GSSM begins to function in its new role as the interim primary GSSM and is now fully functional. You may now access the GUI.

Reversing the Roles of the Interim Primary and Standby GSSM Devices

When the original primary GSSM is available for use in the network, reverse the roles of the two GSSM devices back to the original GSS network deployment.

Note If your original primary GSSM has been replaced by Cisco Systems, see the "Replacing the Primary GSSM with an Available GSS" section for details about replacing a primary GSSM with a new GSS device.

To reverse the roles of the interim primary and standby GSSM devices, perform the following steps:

1. Log in to the CLI of the interim primary GSSM and enable privileged EXEC mode.

   ```
   gssm2.example.com> enable
   gssm2.example.com#
   ```

2. If the GUI configuration has changed, perform a full backup of the interim primary GSSM to preserve the current network and configuration settings (see the "Performing a Full Primary GSSM Backup" section in Chapter 7, , Backing Up, Restoring, and Downgrading the GSSM Database).

3. Place the current interim primary GSSM in standby mode to resume its role in the GSS network as the standby GSSM by entering the following command:

   ```
   gssm2.example.com# gssm primary-to-standby
   ```

   Ensure that a minimum of five minutes have passed since the last GUI configuration change before you enter the **gssm primary-to-standby** command to convert the interim primary GSSM back to its role as standby GSSM.

4. Exit from the CLI of the standby GSSM.

5. Log in to the CLI of the primary GSSM from your original network deployment. The CLI prompt appears.

6. Enable privileged EXEC mode on the primary GSSM.

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

7. Return the standby GSSM to its role as the original primary GSSM in the GSS network by entering the following command:

```
gssm1.example.com# gssm standby-to-primary
```

Note After entering the **gssm primary-to-standby** command, you should ensure that at least 1 minute passes before you enter the **gssm standby-to-primary** command in order to allow time for proper GSS device synchronization.

Configuration changes do not take effect immediately. It may take up to 10 minutes before the other GSS devices in the network learn about the new primary GSSM.

You can now use the primary GSSM as in the original GSS network deployment.

Displaying GSS System Configuration Information

The GSS CLI provides a comprehensive set of **show** commands that display GSS configuration information. The **show** commands are available in all CLI modes.

This section contains the following topics:

Displaying Software Version Information

You can display the software version information about the GSS software by using the **show version** command. The syntax for the **show version** command is as follows:

show version [**verbose**]

Specify the **verbose** optional keyword if you want to view detailed GSS software version information.

To display general GSS software version information, enter:

```
gssm1.example.com# show version

Global Site Selector (GSS)
Model Number: GSS-4492-K9
Copyright (c) 1999-2007 by Cisco Systems, Inc.

Version 2.0 (1.0.0)

Uptime: 4 Hours 0 Minutes and 19 seconds
```

To display detailed GSS software version information, enter:

```
gssm1.example.com# show version verbose

Global Site Selector (GSS)
Model Number: GSS-4490-K9
Copyright (c) 1999-2003 by Cisco Systems, Inc.

Version 1.3(1)

Uptime: 23 Hours 57 Minutes and 53 seconds

Full Version: 1.3(1.0.0)
Compiled on Wed Feb 15 05:51:07 2006 by ralexand from gss-builder -
changeset 26190

Processor 0: Pentium III (Coppermine)  GenuineIntel
Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 02)
Ethernet controller: Intel Corporation 82557 [Ethernet Pro 100] (rev
08)
Ethernet controller: Intel Corporation 82557 [Ethernet Pro 100] (rev
08)
IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 01)
ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 02)
```

```
PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev
03)
SCSI storage controller: Symbios Logic Inc. (formerly NCR) 53c895 (rev
02)
USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 01)
VGA compatible controller: Chips and Technologies F69000 HiQVideo (rev
64)

0000-001f : dma1 | 0020-003f : pic1
0040-005f : timer | 0060-006f : keyboard
0070-007f : rtc | 0080-008f : dma page reg
00a0-00bf : pic2 | 00c0-00df : dma2
00f0-00ff : fpu | 02f8-02ff : serial(auto)
03d4-03d5 : cga | 03f8-03ff : serial(auto)
6c00-6c7f : ncr53c8xx | 7000-701f : Intel Speedo3 Ethernet
7400-741f : Intel Speedo3 Ethernet | fc00-fc07 : ide0
fc08-fc0f : ide1 |
gssm1.example.com: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: IBM      Model: IC35L018UCD210-0 Rev: S5BS
  Type:   Direct-Access                    ANSI SCSI revision: 03
```

Displaying License Information

You can display information about installed GSS licenses by using the **show license** command and its options.

To obtain a listing of the currently-active license modules, enter:

```
gssm1.example.com# show license active
Enabled modules are
DDoS
```

To see which license files are installed, enter:

```
gssm1.example.com# show license installed
License modules are
DDoS
CNR
```

To obtain a complete listing of the license files, enter:

```
gssm1.example.com# show license file-name list
ddos_new.lic
```

To obtain specific license file details, enter:

```
gssm1.example.com# show license file-name ddos_new.lic
FEATURE ddos cisco 1 permanent uncounted HOSTID=ANY \
NOTICE="<LicFileID>ddos_new.lic</LicFileID><LicLineID>0</LicLineID> \
<PAK>1XIOS2C84AB</PAK>" SIGN=CFF95D462F42
```

To obtain a complete picture of the licenses installed in the GSS network from the primary GSS, enter:

```
gssm1.example.com# show license gss-all
Own (Primary GSS) info :
Pak number is :
    1XIOS2C81AB
DDoS Installed, Active
CNR Installed, Active

Other GSS info :

Address : 2.7.0.2
Pak number are :
    1XIOS2C87AB
DDoS Installed, Active
CNR Installed, Active

Address : 2.3.0.2
Pak number is:
    1XIOS2C83AB
DDoS Installed, Active
CNR Installed, Active
```

Displaying Memory Information

You can display information about the GSS memory blocks and statistics by using the **show memory** command.

```
gssm1.example.com# show memory
```

Table 2-1 describes the fields in the **show memory** output.

Table 2-1 Field Descriptions for show memory Command

Field	Description
Memory:	
total	Total usable megabytes of RAM on the GSS.

Table 2-1 Field Descriptions for show memory Command

Field	Description
free	Available megabytes of RAM on the GSS.
Mem:	
total	Total usable megabytes of RAM on the GSS.
used	Currently used RAM.
free	Currently available RAM.
shared	Memory shared between processes, always 0 (zero).
buffers	Memory allocated as the internal kernel buffer space.
cached	Memory allocated for the internal caching of file system data. This memory is reclaimed as needed.
Swap:	
total	Total megabytes of swap space on the GSS.
used	Currently used swap space.
free	Currently available swap space.

Displaying Boot Configuration

You can display information about the GSS software, such as the current boot image and boot device information, by using the **show boot-config** command.

```
gssm1.example.com# show boot-config
```

Table 2-2 describes the fields in the **show boot-config** output.

Table 2-2 Field Descriptions for show boot-config Command

Field	Description
Boot Device	Physical device used to boot the GSS software.
Timeout	Length of time that the Linux boot manager, LILO (Linux Loader) waits to receive an input before automatically booting the GSS device.

Table 2-2 Field Descriptions for show boot-config Command

Field	Description
Label	GSS software version that appears at the LILO prompt.
GSS Software Version	Current GSS software version associated with the Label.
Root Partition	Device used for the Linux root partition (the core of the Linux file system).
Linux Kernel	Version of the Linux kernel used by the GSS software image.
Default Boot Image	Listed software version of the default boot image for the GSS device.

Displaying GSS Processes

You can display a list of internal GSS device processes by using the **show processes** command.

```
gssm1.example.com# show processes
```

Table 2-3 describes the fields in the **show processes** output.

Table 2-3 Field Descriptions for show processes Command

Field	Description
Name	Name of the GSS subsystem, per operating system process.
PID	Process identifier.
MEM	Percentage of memory used by the process.
CPUTIME	Amount of CPU time used since the start of the process.
START	Date or time when the process started.

Displaying System Uptime

You can display the length of time that the GSS has been running by using the **show uptime** command.

```
gssm1.example.com# show uptime
Uptime: 12 Days 18 Hours 5 Minutes and 12 seconds
```

Displaying Disk Information

You can view general information about the GSS hard disk by using the **show disk** command. The general hard disk information includes the available user space on the disk, the size of the database, and the free space available on the disk.

```
gssm1.example.com# show disk
```

Table 2-4 describes the fields in the **show disk** output.

Table 2-4 Field Descriptions for show disk Command

Field	Description
Size	Total size of the disk, in megabytes.
Used	Used space on the disk, in megabytes.
Free	Available space on the disk, in megabytes.
User Space	Disk space allocated to the GSS users.
Database	Disk space allocated to the database configuration.
Safe Storage	Disk space allocated for system data storage.

Displaying UDI Data

You can display GSS Unique Device Identifier (UDI) data by using the **show inventory** command.

```
gssm1.example.com# show inventory
NAME: Chassis, DESCR: Global Site Selector 4492
PID: GSS-4491-K9 , VID: V01, SN: QTFNZD606000011
```

The UDI provides a hardware product identification standard that is a consistent feature across Cisco products, allowing customers to uniquely identify and track Cisco products through their business and network operations. The UDI is composed of three separate data elements which are physically attached to each part:

- Orderable product identifier (PID)
- Version identifier (VID)
- Serial number (SN) of the hardware

The name of the device and a device description are also included in the output of the **show inventory** command.

Displaying System Status

You can display a report on the current operating status of your GSS device, including the online status, current software version, and start date or time for the various components by using the **show system-status** command.

Note The equivalent command to show GSS system status is **gss status**.

```
gssm1.example.com# show system-status
Cisco GSS - 1.3(1) GSS Manager - primary [Wed Feb 15 16 16:37:37 UTC
2006]

Normal Operation [runmode = 5]

START  SERVER
 Aug06  Boomerang
 Aug06  Config Agent (crdirector)
 Aug06  Config Server (crm)
 Aug06  DNS Server
 Aug06  Database
 Aug06  GUI Server (tomcat)
 Aug06  Keepalive Engine
 Aug06  Node Manager
 Aug06  Proximity
 Aug06  Sticky
 Aug06  Web Server (apache)
```

Displaying GSS Services

You can display the current state of the GSS services, such as FTP, NTP, SSH, TACACS+, Telnet, and SNMP by using the **show services** command.

```
gssm1.example.com(config)# show services
 START  SERVICE
 Jul23  Ftp
 Jul23  Ntp
 11:08  Snmp
 14:47  Ssh
 Jul23  Syslog
 Jul23  Tacacs Stats
 Jul23  Telnet
```