Cisco Global Site Selector Getting Started Guide

Software Version 2.0
March 2007

C O N T E N T S

Preface

This guide aids you in setting up and configuring your Cisco Global Site Selector (GSS) and connecting it to the network. After you configure and create your primary GSSM, standby GSSM, and GSS devices to connect to your GSS network, you can begin configuring request routing and global server load balancing.

Certain GSS network management tasks, such as initial device setup, require that you use the command-line interface (CLI) of each GSS device to independently configure the GSS. Other tasks, such as activating GSS devices in the GSS network, require that you use the graphical user interface (GUI) of the primary GSSM to globally configure all GSS devices in a GSS network.

The chapters in this guide describe how to perform the initial setup and configuration tasks of GSS devices in your GSS network. You are instructed to perform the initial setup and configuration tasks at either the CLI of each GSS device or at the GUI of the primary GSSM.

Note To perform global server load-balancing configuration and monitoring, in most cases you have the option of using either the CLI or the GUI at the primary GSSM. For tasks that you can perform using the CLI or the GUI of the primary GSSM, choosing when to use the CLI or the GUI is a matter of personal or organizational choice. However, not every GSLB configuration and monitoring task is available from the GUI or the CLI of the primary GSSM as outlined in Table 1-2 of Chapter 1, Using the CLI and GUI to Manage a GSS Network.

This preface contains the following sections:

- Audience

- How to Use This Guide

- Related Documentation

- Symbols and Conventions

- Obtaining Documentation, Obtaining Support, and Security Guidelines

Audience

To use this guide, you should be familiar with the Cisco Global Site Selector hardware, which is discussed in the *Global Site Selector Hardware Installation Guide*. In addition, you should be familiar with basic TCP/IP and networking concepts, router configuration, Domain Name System (DNS), the Berkeley Internet Name Domain (BIND) software or similar DNS products, and the specific network configuration of your organization.

How to Use This Guide

This guide includes the following chapters:

Chapter/Title	Description
Chapter 1, Using the CLI and GUI to Manage a GSS Network	Provides an overview on when to use the CLI of each GSS device, the CLI of the primary GSSM, and the GUI of the primary GSSM to setup, configure, or perform global server load balancing and monitoring tasks.
Chapter 2, Configuring the GSS Using the CLI Setup Script	Describes how to use the setup script to configure the GSS device. The setup script initiates automatically when you log in and the CSS does not detect an existing startup-configuration file.
Chapter 3, Accessing the GSS CLI	Describes how to access the GSS CLI by making a direct connection to the GSS device using a dedicated terminal or by establishing a remote connection using Telnet or Secure Shell (SSH) from a PC.
Chapter 4, Setting Up Your GSS from the CLI	Describes how to individually configure each GSS device in your GSS network.
Chapter 5, Activating GSS Devices from the GUI	Describes how to activate your standby GSSM and GSS devices from the primary GSSM graphical user interface.
Chapter 6, Activating GSS Devices from the CLI	Describes how to activate GSS devices from the primary GSSM CLI.
Chapter 7, Global Server Load Balancing Summary	Summarizes the individual procedures that you perform from the primary GSSM to configure request routing and global server load balancing on your GSS network.

Related Documentation

In addition to this document, the GSS documentation set includes the following:

Document Title	Description
Global Site Selector Hardware Installation Guide	Information on installing your GSS device and getting it ready for operation. It describes how to prepare your site for installation, how to install the GSS device in an equipment rack, and how to maintain and troubleshoot the GSS hardware.
Regulatory Compliance and Safety Information for the Cisco Global Site Selector	Regulatory compliance and safety information for the GSS.
Release Note for the Cisco Global Site Selector	Information on operating considerations, caveats, and new CLI commands for the GSS software.
Cisco Global Site Selector Administration Guide	Provides the procedures necessary to properly set up, manage, and maintain your GSSM and GSS devices, including login security, software upgrades, GSSM database administration, and logging.
Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide	Procedures on how to configure your primary GSSM from the GUI to perform global server load-balancing, such as configuring source address lists, domain lists, answers, answer groups, DNS sticky, network proximity, and DNS rules. This document also provides an overview of the GSS device and global server load balancing as performed by the GSS.

Document Title	Description
Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide	Procedures on how to configure your primary GSSM from the CLI to perform global server load-balancing, such as configuring source address lists, domain lists, answers, answer groups, DNS sticky, network proximity, and DNS rules. This document also provides an overview of the GSS device and global server load balancing as performed by the GSS.
Cisco Global Site Selector Command Reference	An alphabetical list of all GSS command-line interface (CLI) commands including syntax, options, and related commands. This document also describes how to use the CLI .

Symbols and Conventions

This guide uses the following symbols and conventions to emphasize certain information.

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Variables for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{**x**	**y**	**z**}	Alternative keywords are grouped in braces and separated by vertical bars.
[**x**	**y**	**z**]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.

Screen examples use the following conventions:

screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in **boldface screen** font.
italic screen font	Variables for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Graphical user interface elements use the following conventions:

boldface text	Instructs the user to enter a keystroke or act on a GUI element.
Courier text	Indicates text that appears in a command line, including the CLI prompt.
Courier bold text	Indicates commands and text you enter in a command line.
italic text	Directories and filenames are in *italic* font.

⚠
Caution   A caution means that a specific action you take could cause a loss of data or adversely impact use of the equipment.

Note A note provides important related information, reminders, and recommendations.

1. A numbered list indicates that the order of the list items is important.

    a. An alphabetical list indicates that the order of the secondary list items is important.

- A bulleted list indicates that the order of the list topics is unimportant.

    – An indented list indicates that the order of the list subtopics is unimportant.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

C H A P T E R 1

Using the CLI and GUI to Manage a GSS Network

The Global Site Selector (GSS) has a command-line interface (CLI) and the primary GSSM has both a CLI and a graphical user interface (GUI) that you use to configure the GSS device. This chapter describes when to use the CLI of each GSS device, the CLI of the primary GSSM, or the GUI of the primary GSSM in your GSS network. It also summarizes when to use the following:

- The CLI of each GSS device to perform network setup and configuration tasks.
- The GUI of the primary GSSM to perform network setup and configuration tasks.
- The CLI or the GUI of the primary GSSM to perform global server load-balancing (GSLB) configuration and monitoring tasks.

This chapter contains the following sections:

- CLI and GUI Network Management Overview
- Summary of Tasks Using the CLI and the GUI

CLI and GUI Network Management Overview

Global Site Selectors work together in a GSS network to provide distributed and redundant GSLB DNS services. You accomplish the creation of GSLB DNS services by first performing a basic configuration of each individual device, and then accessing the primary Global Site Selector Manager (GSSM) to manage the centralized and shared GSLB configuration.

The first GSS you configure and create in a GSS network is the primary GSSM. After performing a basic setup of the primary GSSM, you can then add additional GSS devices, including a standby GSSM, or continue directly to configuring GSLB. All GSS devices in your GSS network share the same GSLB configuration as managed by the primary GSSM. When you later add a GSS to the GSS network, the GSS device automatically receives the current GSLB configuration.

Certain GSS network management tasks, such as initial device setup, require that you use the CLI of each GSS device to independently configure the GSS. Other tasks, such as activating GSS devices in the GSS network, require that you use the GUI of the primary GSSM to globally configure all GSS devices in a GSS network.

When you perform global server load-balancing configuration and monitoring tasks, in most cases you have the option to use either the CLI or the GUI of the primary GSSM. For tasks that you can perform using either the CLI or the GUI of the primary GSSM, choosing when to use the CLI or the GUI is a matter of personal or organizational choice. Additionally, you have the option to create your GSLB configuration using one method, and then modify the configuration using the alternate method.

Not every GSLB configuration and monitoring task is available from the GUI and the CLI of the primary GSSM. A few examples include the following:

- Configure sticky and proximity groups using the CLI of the primary GSSM
- Create DNS view filters using the GUI of the primary GSSM
- Perform sticky database and proximity database management using the CLI of each GSS device
- Configure DDoS detection and mitigation using the CLI of each GSS device

Proceed to the "Summary of Tasks Using the CLI and the GUI" section for a detailed overview of the setup, configuration, and global server load-balancing configuration and monitoring tasks that you can perform, and which user interfaces (GUI or CLI) are available for each task.

Summary of Tasks Using the CLI and the GUI

Table 1-1 provides an overview of different configuration tasks that you need to perform. This table identifies the configuration task, the GSS device that you use to perform the task, and which method to use (GUI or CLI) to perform each task. This table also identifies the guide in the GSS documentation set that contains the procedural information.

Table 1-1   Using the CLI or GUI to Perform Configuration Tasks

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Related Document	
				Cisco Global Site Selector Getting Started Guide Chapter	Cisco Global Site Selector Administration Guide
Automatically configure a new GSS using the setup script	Yes	Yes	—	Chapter 2, Configuring the GSS Using the CLI Setup Script	—
Enable remote access	Yes	Yes	—	Chapter 3, Accessing the GSS CLI	—
Manually configure a GSS using the individual CLI setup commands	Yes	Yes	—	Chapter 4, Setting Up Your GSS from the CLI	—
Configure and register a new GSS or standby GSSM with the primary GSSM	Yes	Yes	—	Chapter 4, Setting Up Your GSS from the CLI	—
Activate a new GSS or standby GSSM from the primary GSSM GUI	—	—	Yes	Chapter 5, Activating GSS Devices from the GUI	—

Table 1-1   Using the CLI or GUI to Perform Configuration Tasks (continued)

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Related Document	
				Cisco Global Site Selector Getting Started Guide Chapter	Cisco Global Site Selector Administration Guide
Activate a new GSS or standby GSSM from the primary GSSM CLI	—	—	Yes	Chapter 6, Activating GSS Devices from the CLI	—
Delete GSS devices from the GSS network	—	—	Yes	—	Yes
Change the role of a primary GSSM in the GSS network	Yes (Standby GSSM Only)	Yes	—	—	Yes
Start, stop, reload, or shut down a GSS device	Yes	Yes	—	—	Yes
Install GSS software licenses	Yes	Yes	—	—	Yes
Manage GSS files	Yes	Yes	—	—	Yes
Create and manage CLI user accounts	Yes	Yes	—	—	Yes
Create and manage primary GSSM GUI user accounts (including user roles)	—	—	Yes	—	Yes
Create user views	—	—	Yes	—	Yes
Manage user accounts through a TACACS+ server	Yes	Yes	—	—	Yes
Configure access lists and filter GSS traffic	Yes	Yes	—	—	Yes
Configure SNMP	Yes	Yes	—	—	Yes

Table 1-1   Using the CLI or GUI to Perform Configuration Tasks (continued)

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Related Document	
				Cisco Global Site Selector Getting Started Guide Chapter	Cisco Global Site Selector Administration Guide
Configure device logging	Yes	Yes	—	—	Yes
View centralized system logs in system.log file	—	—	Yes	—	Yes
Back up the primary GSSM	—	Yes	—	—	Yes
Perform GSS software upgrades or downgrades	Yes	Yes	—	—	Yes

Table 1-2 provides an overview of different global server load-balancing (GSLB) configuration and monitoring tasks. This table identifies the GSLB configuration task, the GSS device that you use to perform the task, and which method to use (GUI or CLI) to perform each task. This table also identifies the guide in the GSS documentation set that contains the GSLB procedural information.

Table 1-2   Using the CLI or GUI to Perform GSLB Configuration Tasks

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Related Document	
				Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide	Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide
Export and import GSLB configurations in text format	—	Yes	—	Yes	—
Configure locations, regions, and owners	—	Yes	Yes	Yes	Yes

Table 1-2   Using the CLI or GUI to Perform GSLB Configuration Tasks (continued)

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Related Document	
				Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide	Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide
Configure source address lists	—	Yes	Yes	Yes	Yes
Configure domain lists	—	Yes	Yes	Yes	Yes
Configure keepalives	—	Yes	Yes	Yes	Yes
Configure answers and answer groups	—	Yes	Yes	Yes	Yes
Create DNS rules	—	Yes	Yes	Yes	Yes
Suspend and reactivate a DNS rule	—	—	Yes	—	Yes
Create DNS rules using the DNS Rule Wizard	—	—	Yes	—	Yes
Configure and use DNS rule filters	—	—	Yes	—	Yes
Configure DNS sticky	—	Yes	Yes	Yes	Yes
Create sticky groups	—	Yes	—	Yes	Yes
Perform sticky database management	Yes	Yes	—	Yes	Yes
Configure network proximity (including zones)	—	Yes	Yes	Yes	Yes
Create proximity groups	—	Yes	—	Yes	Yes
Add proximity database entries	Yes	Yes	—	Yes	Yes

Table 1-2   Using the CLI or GUI to Perform GSLB Configuration Tasks (continued)

Task	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide	Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide
				Related Document	
Perform proximity database management	Yes	Yes	—	Yes	Yes
Configure DDoS detection and mitigation	Yes	Yes	—	Yes	—
Monitor individual GSS device status	Yes	Yes	Yes	Yes	Yes
Monitor the GSS network	—	—	Yes	Yes	Yes
Export or print GSSM data	—	—	Yes	—	Yes

C H A P T E R **2**

Configuring the GSS Using the CLI Setup Script

The setup script initiates automatically when you log in and the GSS does not detect an existing startup-configuration file. This chapter describes how to use the setup script to configure a Global Site Selector (GSS) as a primary Global Site Selector Manager (GSSM), standby GSSM, or as a GSS device.

The script configuration process described in this chapter is identical to the script configuration process performed using the **setup** CLI command. If you choose to bypass the setup script, access the GSS CLI as described in Chapter 3, Accessing the GSS CLI, and configure the GSS from the CLI as described in Chapter 4, Setting Up Your GSS from the CLI.

This chapter contains the following sections:

- Using the Setup Script
- Where to Go Next

Using the Setup Script

When you boot the GSS platform for the first time and the GSS does not detect a startup-configuration file, a setup script guides you through the process of initially configuring the GSS. The script includes these steps:

- Specifying a hostname for the GSS device
- Configuring Ethernet 0 and Ethernet 1
- Configuring a default gateway

- Entering the IP addresses of the name servers (a maximum of eight)

- Configuring a remote access protocol (FTP, Telnet, or SSH) so that you can administer the GSS device remotely in the future

The GSS provides a default answer in brackets [ ] for each question in the setup script. To accept the default configuration, press **Enter**, and the GSS accepts the setting.

The script configuration process described in this section is identical to the script configuration process performed using the **setup** CLI command.

To configure a GSS device from the setup script, perform the following steps:

1. You must have physical access to the GSS device to configure it from the setup script. If you have not already done so, connect a console or terminal to the Console port on the GSS device. Refer to the *Cisco Global Site Selector Hardware Installation Guide* for instructions on connecting a console cable to your Cisco GSS series hardware.

2. Press the power control button on the GSS and the boot process occurs. See the *Cisco Global Site Selector Hardware Installation Guide* for details.

3. At the prompt "Do you want to continue? (y/n) [no]:", type **y** to continue the setup (or press **Enter** to accept the default and bypass the setup script).

    If you choose to bypass the setup script at this point, you can either:

    – Manually configure the GSS from the CLI as described in Chapter 4, Setting Up Your GSS from the CLI.

    – Use the **setup** CLI command at a later point in time to configure basic configuration information (as described in this procedure). You cannot enter the **setup** command while running GSS software. Enter the **gss stop** command to stop the GSS software before entering the **setup** command.

4. At the Hostname prompt, specify a qualified hostname for the GSS device. A fully qualified hostname requires at least one period "." in the name, as in this example:

    ```
    Enter the Hostname of this device: gssm1.example.com
    ```

5. At each Interface eth0 and eth1 prompt, activate the Ethernet interface and then specify the IP address and subnet mask for each interface.

```
* Interface eth1 (Inactive)
Do you want to change this? (y/n) [n]: y
Do you want to activate this interface? (y/n) [n]: y
Enter the IP address: 192.168.1.3
Enter the netmask: 255.255.255.0
```

After you run the setup script you can specify additional configuration parameters for each Ethernet interface using the **interface ethernet** CLI command (such as the **autosense**, **duplex**, and **speed** options). Refer to Chapter 4, Setting Up Your GSS from the CLI for detailed information on the **interface ethernet** command.

6. At the default gateway prompt, enter gateway information for the GSS device:

```
Do you want to configure a default gateway? (y/n) [y]: y
Enter the default gateway [192.16.86.1]: 192.16.86.6
```

7. At the Name Servers prompt, configure the domain name server or servers to be used by the GSS device. You can enter individual addresses or specify a maximum of eight name servers in a list. Enter a hyphen ('-') at a blank entry to instruct the GSS to stop requesting name servers.

```
Enter the IP addresses for up to 8 Name Servers.
Enter a dash ('-') at a blank entry to stop entering Name Servers.
At least one Name Server is required for this setup script.
Enter Name Server 1 [172.16.124.122]: 172.16.12.1
Enter Name Server 2: 192.168.1.2
Enter Name Server 3: -
```

8. At the Remote Access prompt, activate the remote access protocol required for the GSS device.

```
* Remote Access
Do you want to enable FTP access? (y/n) [y]: n
Do you want to enable Telnet access? (y/n) [n]: y
Do you want to enable SSH access? (y/n) [y]: y
```

The setup script guides you through a series of questions about configuring the device as a GSSM (primary or standby) or as a GSS.

9. Perform one of the following actions:

- The primary GSSM performs content routing as well as centralized management functions for the GSS network. The primary GSSM serves as the organizing point of the GSS network. To configure the device as the primary GSSM, perform the following steps:

    a. At the prompt "Do you want to configure this GSS as a Manager (gssm)? (y/n) [y]:", type **y**.

    b. At the prompt "Do you want to configure this GSSM as the Primary? (y/n) [y]:", type **y**.

- The standby GSSM performs GSLB functions for the GSS network while operating in standby mode. In addition, the standby GSSM can be configured to act as the GSSM should the primary GSSM need to go offline for repair or maintenance. To configure the device as the standby GSSM perform the following steps:

    a. At the prompt "Do you want to configure this GSS as a Manager (gssm)? (y/n) [y]:", type **y**.

    b. At the prompt "Do you want to configure this GSSM as the Primary? (y/n) [y]:", type **n**.

    c. At the prompt "Enter the Hostname or IP address of the Primary GSSM []:" specify the hostname or IP address of the primary GSSM for your network.

- The GSS performs routing of DNS queries based on DNS rules and conditions configured using the primary GSSM. Each GSS is known to and synchronized with the primary GSSM. To configure the device as a GSS, perform the following steps:

    a. At the prompt "Do you want to configure this GSS as a Manager (gssm)? (y/n) [y]:", type **n.**

    b. At the prompt "Enter the Hostname or IP address of the Primary GSSM []:", specify the hostname or IP address of the primary GSSM for your network.

10. When finished, perform one of the following actions as prompted by the software:

- Apply as the Running Configuration—Apply the setup script configuration changes to the running-configuration file.

- Edit This Configuration—Return to the beginning of the setup script and edit specific configuration information.

- Discard Configuration and Quit Setup—Cancel making initial configuration changes.

Where to Go Next

After you complete running the setup script, you may proceed to one of the following sections in this guide:

- To access the CLI using a direct serial connection or to reconfigure remote access login, proceed to Chapter 3, Accessing the GSS CLI

- To perform additional GSS setup using the GSS CLI (such as setting the system clock and adjusting Ethernet interface parameters), proceed to Chapter 4, Setting Up Your GSS from the CLI.

- To access the primary GSSM GUI to activate and configure your GSS devices, proceed to Chapter 5, Activating GSS Devices from the GUI.

- To activate and configure your GSS devices from the CLI, proceed to Chapter 6, Activating GSS Devices from the CLI.

- To configure your GSS devices and resources from the primary GSSM for global server load-balancing, proceed to Chapter 7, Global Server Load Balancing Summary.

Accessing the GSS CLI

You can access the GSS CLI in one of the following ways:

- Making a direct connection to the GSS device using a dedicated terminal.
- Establishing a remote connection using the Secure Shell (SSH), Telnet, or FTP protocols from a PC.

This chapter contains the following sections:

- Accessing the CLI Using a Direct Serial Connection
- Logging in to the CLI and Enabling Privileged EXEC Mode
- Remotely Accessing a GSS Device
- Where to Go Next

Accessing the CLI Using a Direct Serial Connection

To access the GSS CLI by using a serial connection, establish a direct serial connection between your terminal and the GSS device. For information on how to establish a serial connection with your device, see the *Cisco Global Site Selector Hardware Installation Guide.*

Once connected, use any terminal communications application to access the GSS CLI. The following procedure uses HyperTerminal for Windows.

To access the GSS CLI using a direct serial connection, perform the following steps:

1. Launch HyperTerminal. The Connection Description window appears.

2. Enter a name for your session in the Name field.

3. Click **OK**. The Connect To window appears.

4. From the drop-down list, choose the COM port to which the device is connected.

5. Click **OK**. The Port Properties window appears.

6. Set the port properties:
   – Baud Rate = 9600
   – Data Bits = 8
   – Flow Control = none
   – Parity = none
   – Stop Bits = 1

7. Click **OK** to connect.

8. Press **Enter** to display the CLI prompt.

Once a session is created, choose **Save As** from the File menu to save the connection description. Saving the connection description has the following two advantages:

- The next time you launch HyperTerminal, the session is listed as an option under **Start** > **Programs** > **Accessories** > **HyperTerminal** > **Name_of_session**. This option lets you reach the CLI prompt directly without going through the configuration steps.

- You can connect your cable to a different device without configuring a new HyperTerminal session. If you use this option, make sure that you connect to the same port on the new device that you configured in the saved HyperTerminal session. Otherwise, a blank screen appears without a prompt.

Logging in to the CLI and Enabling Privileged EXEC Mode

After you make a direct connection to the GSS device using a dedicated terminal, log in to a GSS device and enable privileged EXEC mode at the CLI. To do so, 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. Specify your GSS administrative username and password to log in to the GSS device. If this is your first time logging in to the GSS, use the default account name (admin) and password (default) to access the CLI.

   The CLI prompt appears.

   ```
   localhost.localdomain>
   ```

3. 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 (#).

Remotely Accessing a GSS Device

To monitor the performance of your GSS devices and administer those devices once deployed, you require remote access to those devices. Once you have basic network connectivity on the GSS device, you may use the CLI to enable remote access to each device using the Secure Shell (SSH), Telnet, or FTP protocols.

We recommend using an SSH connection because SSH provides secure communication over insecure channels and provides strong authentication. The GSS supports remote login to the GSS over an SSH session that uses private and public key pairs for authentication.

You must have physical access to the GSS device to set up remote access by Telnet or SSH connection. See the *Cisco Global Site Selector Hardware Installation Guide* for instructions on connecting a console cable to your Cisco Global Site Selector series hardware.

This section contains the following topics:

Enabling Remote Access on a GSS Device

To enable SSH, Telnet, or FTP on your GSS device, perform the following steps:

1. Log on to the GSS and enable privileged EXEC mode as described in the "Logging in to the CLI and Enabling Privileged EXEC Mode" section.

2. Enable global configuration mode on the device.

```
localhost.localdomain# config
localhost.localdomain(config)#
```

3. To enable Secure Shell (SSH) connections to the GSS device, use the **ssh enable** command. SSH on the GSS supports the SSH v2 and v1 protocols. For SSH v2, the software provides 128-bit AES, Blowfish, 3DES, CAST128, Arcfour, 192-bit AES, or 256-bit AES. For SSH v1, the software provides encrypted communication using ciphers such as 3DES or Blowfish.

```
localhost.localdomain(config)# ssh enable
```

By default, the GSS turns off SSH protocol v1 because it is considered to be cryptographically insecure. If your remote SSH application cannot support SSH protocol v2 and requires SSH protocol v1, enter the following command to enable SSH protocol version 1 for the GSS:

```
localhost.localdomain(config)# ssh protocol version 1
```

> **Note**   If your clients support both SSH protocol v2 and v1, we recommend that you configure the client to use SSH protocol v2 by default.

To disable SSH, use the **no** form of this command.

```
localhost.localdomain(config)# no ssh enable
```

4. To enable Telnet on the selected GSS device and to establish a Telnet connection, use the **telnet** command. The syntax for the **telnet** command is as follows:

telnet {**enable** | {*ip_or_host*} | [*port*]

The keywords and arguments are as follows:

- *ip_or_host*—Specifies the IP address or hostname of the device with which you want to establish a Telnet connection. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).

- *port*—(Optional) Allows you to change the port number for the Telnet session to a port other than 23 (the Telnet port). Enter a number from 1 to 65535. The default is 23.

For example, to launch Telnet and establish a connection to the device at IP address 192.168.2.3, enter:

```
localhost.localdomain(config)# telnet enable
localhost.localdomain# telnet 192.168.2.3
```

To disable Telnet on your GSS device, use the **no** form of this command.

```
localhost.localdomain(config)# no telnet enable
```

5. To enable the File Transfer Protocol (FTP) or launch an FTP session on your GSS device, use the **ftp enable** command.

ftp enable | *ip_or_host*

The *ip_or_host* option specifies the IP address or hostname of the FTP server you want to access. Be sure to enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).

For example, to launch the FTP session and access the device at IP address 192.168.0.1, enter:

```
localhost.localdomain(config)# ftp enable
localhost.localdomain(config)# ftp 192.168.0.1
```

To disable FTP on your GSS device or remove the IP address from the FTP server, use the **no** form of this command.

```
localhost.localdomain(config)# no ftp enable
localhost.localdomain(config)# no ftp 192.168.0.1
```

6. To enable access to an FTP client for different types of users, use the **ftp-client enable** command.

ftp-client enable {*all* | *admin*}

The *all* option enables FTP client access for all users, while the *admin* option enables FTP client access for administrative users only. For example:

```
localhost.localdomain(config)# ftp-client enable all
localhost.localdomain(config)# ftp-client enable admin
```

To remove a specific FTP client configuration and return to the default disabled state, use the **no** form of this command.

```
localhost.localdomain(config)# no ftp-client enable all
```

7. Save your configuration changes to memory.

```
localhost.localdomain(config)# copy running-config startup-config
```

8. Exit global configuration mode.

```
localhost.localdomain(config)# exit
localhost.localdomain#
```

Note the following SSH, Telnet, and FTP remote access considerations:

- The GSS supports a maximum limit of 40 concurrent Telnet or FTP sessions within a 60-second window. The GSS can receive additional concurrent Telnet and FTP connections that are made outside of a 60-second window.

- The GSS supports a maximum limit of 250 SSH connections. When the GSS reaches this limit, the Connection terminated on signal 13 message appears at the CLI of the computer where you initiated the SSH session to the GSS.

To view the operating status of the remote access protocol (SSH, Telnet, or FTP) on your GSS device, enter the following commands:

- To view if FTP and the FTP client are enabled for the GSS device, enter:

```
localhost.localdomain# show ftp
ftp is enabled
ftp-client is enabled for all users
```
- To view if Telnet is enabled for the GSS device, enter:

```
localhost.localdomain# show telnet
telnet is enabled
```

- To view if SSH is enabled for the GSS device, enter:

```
localhost.localdomain# show ssh
ssh is enabled
```

Accessing the CLI Using a Remote Connection

Use either Telnet or SSH from a PC to remotely access the GSS CLI. You cannot connect to more than one device during a single Telnet or SSH session. You can, however, have several Telnet or SSH sessions running in parallel for different devices. Before you attempt to remotely access a GSS device, ensure that you enable Telnet or SSH on that device (see the "Enabling Remote Access on a GSS Device" section).

We recommend using an SSH connection because SSH provides secure communication over insecure channels and provides strong authentication. The GSS supports remote login to the GSS over an SSH session by using a private and public key pair for authentication.

To access the GSS CLI using your preferred SSH or Telnet client, perform the following steps:

1. Enter the hostname or IP address of the GSS or GSSM.

2. Specify your GSS administrative username and password to log in to the GSS device.

Accessing the CLI Over SSH Using a Private and Public Key Pair

The GSS supports remote login to the GSS over an SSH session that uses private and public key pairs for authentication. With this method of remote connection, use a generated private and public key pair to participate in a secure communication by encrypting and decrypting messages. Use of a private and public key pair bypasses the normal username and password authentication process. This remote access method may be useful when running scripts that connect automatically to the GSS.

Generate the private key and the corresponding public key as a key pair on a server separate from the GSS and then use the **scp** command on the GSS to copy the public key to the GSS /home directory. The **scp** command automatically creates an .ssh folder under the GSS /home directory.

By default, the GSS disables SSH key support. As a one-time process, after you initially copy the private and public keys onto the GSS, you must enable global access to those keys to remotely log in to the GSS.

To generate a private and public key pair and copy the keys to the GSS, perform the following steps:

1. Generate the SSH private key and the corresponding SSH public key as a key pair on a server separate from the GSS. See the documentation included with the SSH software for details on generating the private and public key pair.

2. When the SSH private and public key is available, log on to the GSS and enable privileged EXEC mode as described in the "Logging in to the CLI and Enabling Privileged EXEC Mode" section.

3. Use the **scp** command from the GSS to securely copy the generated public key from the server to the GSS /home directory. The **scp** command automatically creates an .ssh folder under the GSS /home directory.

```
localhost.localdomain# scp myusername@1myhost:~/mykey.pub .
myusername@1myhost password:
mykey.pub 100% |****************************| 241 00:00
```

After generating the public key, you may FTP the generated public key to the GSS. In this case, while you are in FTP mode, you must use the **mkdir** command to manually create the .ssh folder on the FTP server.

4. Use the **type** command to append the public key to the /home/.ssh/authorized_keys file, which is a special file that the GSS software looks for when authenticating public/private keys.

```
localhost.localdomain# cd .ssh
localhost.localdomain# type ../mykey.pub >> authorized_keys
```

5. Activate an SSH session from the remote host to the GSS using the private key. For example, on most Unix systems you would enter the following command line:

```
ssh -i private.key gss.cisco.com
```

6. Globally enable remote access to the copied private and public keys on the GSS by entering the following command:

```
localhost.localdomain# config
localhost.localdomain(config)# ssh keys
```

You do not need to enter the **ssh keys** command again for subsequent private and public keys that you copy to the GSS.

Where to Go Next

To configure your GSS device from the CLI and connect it to the GSS network, proceed to Chapter 4, Setting Up Your GSS from the CLI. This process also includes information on how to configure the GSS as a primary GSSM, standby GSSM, or as a GSS device.

If you automatically configured the GSS using the setup script (see Chapter 2, Configuring the GSS Using the CLI Setup Script), you may need to configure additional GSS parameters, such as setting the system clock and adjusting Ethernet interface parameters.

If you do not need to configure additional GSS parameters, access the primary GSSM GUI to activate and configure your GSS devices. Proceed to Chapter 5, Activating GSS Devices from the GUI.

You can also activate and configure your GSS devices from the CLI. To do so, proceed to Chapter 6, Activating GSS Devices from the CLI.

Setting Up Your GSS from the CLI

This chapter describes how to configure your GSS devices from the CLI and connect it to the GSS network. This process describes how to configure the GSS as a primary GSSM, a standby GSSM, or as a GSS device.

This chapter contains the following sections:

- Initial Setup Quick Start
- Logging in to the CLI and Enabling Privileged EXEC Mode
- Setting the System Clock
- Configuring a Hostname for the GSS Device
- Configuring an Ethernet Interface on a GSS Device
- Specifying Name Servers
- Configuring an IP Route for the GSS
- Resolving a Host or Domain Name to an IP Address
- Configuring a Primary GSSM
- Configuring a Standby GSSM
- Configuring a Global Site Selector
- Where to Go Next

Initial Setup Quick Start

Table 4-1 is a quick start configuration table designed to help you configure your GSS quickly from the CLI. This table provides information and examples on the following basic steps to perform the following:

- Configuring the system clock for the GSS device
- Specifying a qualified hostname for the GSS device
- Configuring Ethernet 0 and Ethernet 1
- Configuring a default gateway
- Entering the IP addresses of the name servers (maximum of eight)
- Configuring the primary GSSM, standby GSSM, and GSS devices that comprise your GSS network

Table 4-1   Initial Setup Quick Start

Task and Command Example
1. If you have not already done so, power on and boot the GSS (as described in the *Cisco Global Site Selector Hardware Installation Guide*).
2. If you have not already done so, enable a remote access protocol (such as Telnet or SSH) to access the GSS CLI. See Chapter 3, Accessing the GSS CLI.
3. Log on to the CLI, and at the GSS CLI prompt, enable privileged EXEC mode. `localhost.localdomain> enable` By default, the hostname for GSS devices is localhost.localdomain. This name changes once you configure the hostname for the device.
4. Enable privileged EXEC mode. `localhost.localdomain> enable`
5. Configure the time using the **clock set** command. Enter the time in the *hh*:*mm*:*ss* format and the date in *month dd yyyy* format. `localhost.localdomain# clock set 12:10:05 Feb 15 2006`

Table 4-1   Initial Setup Quick Start (continued)

Task and Command Example

6. (Optional) If you intend to use an NTP server to synchronize the GSS
    system clock, access global configuration mode and specify the NTP server.

    ```
    localhost.localdomain# config
    localhost.localdomain(config)# ntp-server 172.16.1.2 172.16.1.3
    localhost.localdomain(config)# ntp enable
    ```

7. Configure a hostname for the GSS device. The **hostname** command
    requires a fully qualified hostname, which requires at least one period (.) in
    the name.

    ```
    localhost.localdomain(config)# hostname gssm1.example.com
    ```

8. From global configuration mode, enter interface configuration mode and
    configure the attributes of GSS interface Ethernet 0 or Ethernet 1. Each GSS
    device contains two Ethernet interfaces, 0 and 1.

    ```
    gssm1.cisco.com(config)# interface ethernet 0
    gssm1.cisco.com(config-eth0)# speed 100
    gssm1.cisco.com(config-eth0)# duplex full
    ```

    You cannot execute interface commands while the GSS software is running
    (for example, serving DNS requests). You must enter the **gss stop** command
    to stop the GSS software before executing the **interface ethernet** command.

9. Use the **gss-communications** command to configure a GSS Ethernet
    interface as the designated network interface for GSS device
    communication.

    ```
    gssm1.cisco.com(config-eth0)# gss-communications
    gssm1.cisco.com(config-eth0)# exit
    gssm1.cisco.com(config)#
    ```

10. Configure the IP address and subnet mask for the interface.

    ```
    gssm1.cisco.com(config-eth0)# ip address 192.168.3.24
    255.255.255.0
    ```

11. Use the **gss-tcp-keepalives** command to designate either Ethernet 0 or
    Ethernet 1 for TCP and HTTP HEAD keepalive communication.

    ```
    gssm1.cisco.com(config)# interface eth1
    gssm1.cisco.com(config-eth1)# gss-tcp-keepalives
    ```

Table 4-1   Initial Setup Quick Start (continued)

Task and Command Example
12. Exit interface configuration mode. `gssm1.cisco.com(config-eth1)# `**`exit`** `gssm1.cisco.coml(config)#`
13. Define a default gateway for the GSS device. `gssm1.cisco.com(config)# `**`ip default-gateway 172.16.7.18`**
14. Configure the domain name server or servers to be used by the GSS device. You can enter individual IP addresses or specify a maximum of eight name servers using a comma-separated or space-separated list. `gssm1.cisco.com(config)# `**`ip name-server 192.168.12.1,`** **`192.168.12.5, 192.168.12.7`**
15. Exit global configuration mode. `gssm1.cisco.com(config)#`**`exit`**
16. Configure the primary GSSM in your GSS network. You must have a primary GSSM configured and enabled before you can enable a standby GSSM and GSS devices. `gssm1.cisco.com# `**`gss enable gssm-primary`**
17. Configure the standby (backup) GSSM in your GSS network and associate it with the DNS name or IP address of the primary GSSM. The standby GSSM is intended to be a backup device to be used on a temporary basis until the primary GSSM comes back online. `gssm2.example.com# `**`gss enable gssm-standby gssm1.example.com`**
18. Enable each GSS device as a GSS and direct it to the primary GSSM in your GSS network. `gss1.example.com# `**`gss enable gss gssm1.example.com`**
19. Save your configuration changes to memory. `gssm1.example.com# `**`copy running-config startup-config`**

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. 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 Chapter 3, Accessing the GSS CLI.

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 (#).

Setting the System Clock

To set the date, time, or time zone for a GSS device, use the **clock** command. When you enter this command, the GSS device displays the current date and time.

This section contains the following topics:

- Setting the Time and Date
- Setting the Time Zone
- Setting User-Defined Time Zones
- Setting User-Defined Daylight Saving Time
- Setting Daylight Saving Time to Another Predefined Summer Time
- Setting the Hardware Clock
- Showing the Date, Time, and Timezone

Setting the Time and Date

Use the **clock set** command to set the time and the date for a GSS device. Enter the time and date:

- **Time**—Hour, minutes, and seconds as integers in military-time (24-hour) format, separated by colons.
- **Date**—Enter the month, day, and year as integers with colon (:) characters separating them.

The syntax for the **clock set** command is as follows:

> **clock set** *hh:mm:ss MONTH DD YYYY*

The keywords and arguments are as follows:

- **set**—Sets the device clock to the date and time provided.
- *hh:mm:ss*—Current time to which the GSS device clock is being reset. Specify one or two digits for the hours, minutes, and seconds in military-time (24-hour) format, separated by colons.

- *MONTH DD YYYY*—Current date to which the GSS device clock is being reset. Specify the full name of the month, one or two digits for the day, and four digits for the year. The following month names are recognized: January, February, March, April, May, June, July, August, September, October, November, and December.

For example, to specify a time of 12:10 and a date of February 15, 2006, enter:

```
localhost.localdomain# clock set 12:10:05 February 15 2006
```

Note   If you previously enabled NTP on a GSS, the GSS prevents you from using the **clock set** command and displays an error message. If you want to manually set the clock for the GSS, first disable NTP using the **no ntp enable** command before setting the clock. See the "Setting the Hardware Clock" section for more information.

Setting the Time Zone

The time stored in the GSS is the local time. Use the **clock timezone** command to specify a time zone for the GSS, synchronizing the log timestamps to a new timezone. The name of the timezone. Enter **?** to list all supported time zones, countries, continents, and cities.

There are a number of options available to set the local time zone for your GSS:

- Standard time zone (for example, GMT, EST, UTC).
- Country or part of a continent (for example, America, Europe, Egypt)
- Specific city (for example, New York, Paris)

The syntax for this command is as follows:

> **clock timezone** *timezonename*

The *timezonename* is the name of the time zone you specify for the GSS. Enter **?** to list all supported time zone names.

For example, to specify the Greenwich Mean Time (GMT) time zone, enter:

```
localhost.localdomain# clock timezone GMT
```

For example, to specify the time zone to the local time in Paris, enter:

```
localhost.localdomain# clock timezone europe paris
```

Setting User-Defined Time Zones

The **clock user-timezone** command allows you to set user-defined time zones.

The syntax for this command is as follows:

clock user-timezone *timezonenam*e | *hour_offset* <-23,+24> | *minute_offset* <0-59>

The keywords and arguments are as follows:

- *timezonename*—Name of the user-defined time zone.

- *hour_offset*—Hour offset for the user-defined time zone. Valid values range from -23 to +24.

- *minute_offset*—Minute offset for the user-defined time zone. Valid values range from 0 to 59.

Setting User-Defined Daylight Saving Time

The **clock user-summer-time** command allows you to set a user-defined daylight saving time.

The syntax for this command is as follows:

clock user-summer-time *summer-time name* | *start time (hh:mm)* <0-23> | *start day* <Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday> | *start week* <1-5> |
start month <April, August, December, February, January, July, June, March, May, November, October, September>| *end time (hh:mm)* <0-23> |
end day <Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday> | *end week <1-5>* |
end month <April, August, December, February, January, July, June, March, May, November, October, September> | *offset* (in minutes) <0-1440>

The keywords and arguments are as follows:

- *summer-time name*—Name of the user-defined summer time.

- *start time*—Start time for the user-defined summer time in hours and minutes. Valid values are from 0-23.

- *start day*—Start day for the user-defined summer time. Valid values are Friday, Monday, Saturday, Sunday, Thursday, Tuesday, and Wednesday.

- *start week*—Start week for the user-defined summer time. Valid values are from 1-5.

- *start month*—Start month for the user-defined summer time. Valid values are April, August, December, February, January, July, June, March, May, November, October, and September.

- *end time*—End time for the user-defined summer time in hours and minutes. Valid values are from 0-23.

- *end day*—End day for the user-defined summer time. Valid values are Friday, Monday, Saturday, Sunday, Thursday, Tuesday, and Wednesday.

- *end week*—End week for the user-defined summer time. Valid values are from 1-5.

- *end month*—End month for the user-defined summer time. Valid values are April, August, December, February, January, July, June, March, May, November, October, and September.

- *offset*—Offset (in minutes) for the user-defined time zone. Valid values are from 0-1440.

Setting Daylight Saving Time to Another Predefined Summer Time

The **clock summer-time** command allows you to set daylight saving time to another predefined summer time.

The syntax for this command is as follows:

clock summer-time *timezone* <ADT (*Atlantic Daylight Time)* | AKDT *(Alaska Standard Daylight Time)* | CDT *(Central Daylight Time)* | EDT *(Eastern Daylight Time)* | MDT *(Mountain Daylight Time)* | PDT *(Pacific Daylight Time)*

The keywords and arguments are as follows:

- **summer-time**—Allows you to set daylight saving time to another predefined summer time.

- *timezonename*—Name of the other predefined summer time zone. Valid values are ADT *(Atlantic Daylight Time)*, AKDT *(Alaska Standard Daylight Time)*, CDT *(Central Daylight Time)*, EDT *(Eastern Daylight Time)*, MDT *(Mountain Daylight Time)*, and PDT *(Pacific Daylight Time)*

For example, if you wish to set up standard time and daylight saving time in the Eastern Time Zone (that is, Eastern Standard Time (EST) Universal Time Coordinated (UTC -5)) and its daylight saving time (that is, Eastern Daylight Time (EDT) (UTC -4), use the **clock user-timezone**, **summer-time**, and **user-summer-time** commands as shown in Table 4-2.

EDT begins at 2:00 a.m. local time on the first Sunday in April and ends at 2:00 a.m. local time on the last Sunday of October.

Table 4-2   Using the Clock Commands—Example

1. Set the clock based on UTC.

<pre>gss2.gss-tb6.com# **clock set 7:45:00 September 7 2006**
gss2.gss-tb6.com# **show clock**
System time: Thu Sep 7 07:45:05 UTC 2006.</pre>

2. Set the clock to EST by using the **user-timezone** command.

<pre>Timezone set.com# **clock user-timezone EST -5 0**
Please restart the GSS (reload) to sync log timestamps to new
timezone.
gss2.gss-tb6.com# **show clock**
System time: Thu Sep 7 02:45:17 EST 2006</pre>

Note   You need to set the **user-timezone** before using the **summer-time** command.

I

3. Set the summer time on the GSS in one of two ways:

   a. Enter the **summer-time** command.

   ```
   gss1.gss-tb6.com#clock summer-time ?
     ADT   Atlantic Daylight Time: 2 am 1st Sunday April - 2 am last
   Sunday Oct, +60 min
     AKDT  Alaska Standard Daylight Time: 2 am 1st Sunday April - 2
   am last Sunday
   Oct, +60 min
     CDT   Central Daylight Time: 2 am 1st Sunday April - 2 am last
   Sunday Oct, +60 min
     EDT   Eastern Daylight Time: 2 am 1st Sunday April - 2 am last
   Sunday Oct
     MDT   Mountain Daylight Time: 2 am 1st Sunday April - 2 am last
   Sunday Oct, +60 min
     PDT   Pacific Daylight Time: 2 am 1st Sunday April - 2 am last
   Sunday Oct, +60 min
   gss1.gss-tb6.com#clock summer-time EDT
   Timezone set.
   Please restart the GSS (reload) to sync log timestamps to new
   timezone.
   ```

   b. Enter the **user-summer-time** command.

   ```
   gss2.gss-tb6.com# clock user-summer-time EDT 2:00 Sunday 1 April
   2:00 Sunday 5 October 60
   Timezone set.
   Please restart the GSS (reload) to sync log timestamps to new
   timezone.
   gss2.gss-tb6.com# show clock
   System time: Thu Sep  7 03:47:07 EDT 2006
   ```

If you reside in one of the following timezones, ADT, AKDT, CDT, EDT, MDT, or PDT, you use the **clock summer-time** command as shown in step 3a to set the summer-time on the GSS. If you need to configure a custom summer-time, use the **clock user-summer-time** command and follow step 3b instead.

In this example, the summer-times are predefined summer times. After it is finished, the clock will be set back to the user-timezone after the daylight saving time duration is covered. In this particular instance, the time zone will be set back to EST after 2:00 a.m. on the last Sunday in October.

Note You set both the **summer-time** and **user-summer-time** command options with respect to UTC only, and not the **user-timezone**. Also, there is no relation to the **clock timezone** command that was used to establish a time zone on the GSS.

Setting the Hardware Clock

The hardware clock is powered by a Lithium battery on the motherboard of the GSS. The system clock is a software concept, rather than an actual physical entity. It is updated by the Network Time Protocol (NTP) or by the **clock set** command. For more information on NTP, see the "Synchronizing the GSS System Clock with an NTP Server" section, while the "Setting the Time and Date" section contains more information on the **clock set** command.

The **clock update-calendar** and **clock read-calendar** commands provide a way for you to synchronize the hardware clock and the system clock without having to reload the GSS. You use **clock update-calendar** to update the hardware calendar from the system clock and **clock read-calendar** to read the hardware calendar into the system clock.

Specifically, you use **clock update-calendar** when the system clock is set via NTP and you wish to synchronize the system time with the hardware clock. You then use **clock read-calendar** when the system clock is set via NTP and you wish to revert back to using the hardware clock.

The syntax for these commands is as follows:

clock update-calendar

clock read-calendar

For example, to update the hardware calendar from the system clock, enter:

```
localhost.localdomain# clock update-calendar
```

For example, to read the hardware calendar into the system clock, enter:

```
localhost.localdomain# clock read-calendar
```

Synchronizing the GSS System Clock with an NTP Server

NTP enables you to synchronize the GSS system clock to a time server. NTP is a protocol designed to synchronize the clocks of computers over a network. NTP assures accurate local time-keeping with references to radio and atomic clocks. The NTP protocol is capable of synchronizing distributed clocks within milliseconds over long time periods. You can specify a maximum of four NTP servers.

Note If you are using DNS sticky and your network contains multiple GSS devices operating in a global sticky mesh, we strongly recommend that you first synchronize the system clock of each GSS device in the mesh with an NTP server.

Use the **ntp-server** global configuration mode command to specify one or more NTP servers for GSS clock synchronization. To disable an NTP time server, use the **no** form of this command.The syntax for this command is as follows:

ntp-server *ip_or_host*

The *ip_or_host* argument specifies the IP address or hostname of the NTP public time server that provides the clock synchronization. You can specify a maximum of four IP addresses or hostnames. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).

Use the **ntp enable** global configuration mode command to enable the NTP service. To disable NTP, use the **no** form of this command. The syntax of this command is:

ntp enable

For example, to specify the IP addresses of two NTP time servers, enter:

```
localhost.localdomain# config
localhost.localdomain(config)# ntp-server 172.16.1.2 172.16.1.3
localhost.localdomain(config)# ntp enable
```

To view if NTP is enabled for the GSS device, enter:

```
localhost.localdomain# show ntp
Ntp is enabled

ntp-server 172.16.1.2
ntp-server 172.16.1.3
```

To remove a specified NTP server, enter:

```
localhost.localdomain(config)# no ntp-server 172.16.1.3
```

To disable NTP, enter:

```
localhost.localdomain(config)# no ntp enable
```

Showing the Date, Time, and Timezone

Use the **show clock** command to display the current date, time, and timezone name.

```
localhost.localdomain# show clock
System time: Wed February 15 20:55:36 UTC 2006
```

Table 4-3 describes the fields in the **show clock** command output.

Table 4-3   Field Descriptions for the show clock Command

Field	Description
Date	Current date in the format of day, month, and year.
Time	Current time in the format of hour, minute, and second, for example, 16:23:45.
Timezone	Name of the configured time zone.
Year	Current year.

Configuring a Hostname for the GSS Device

By default, the hostname for GSS devices is localhost.localdomain. The hostname is used for the command prompts and default configuration filenames. To configure a qualified hostname for the GSS device, use the **hostname** command. This name changes once you configure the hostname for the device.

The **hostname** command requires a fully qualified hostname, which requires at least one period (.) in the name (for example, hostname.foo.com). The **no** form of this command erases the configured hostname and restores the default value.

When you specify a hostname for a GSS (primary GSSM, standby GSSM, or GSS device) that is operating in a lab network environment, the top-level domain of the hostname cannot begin with a numerical value. For example, you cannot name a primary GSSM as gssm.1lab. If you attempt to create or change a hostname for a top-level domain to a name that begins with a number, the following message appears:

```
Top level domains of hostnames cannot begin with a number
```

For the purposes of GSS interdevice communications, configure the hostname on the same interface (eth0 or eth1) that is being used for GSS communications, as set using the **gss-communications** command.

The syntax for this global configuration mode command is:

> **hostname** *host_name*

Specify the new hostname for the GSS device as a case sensitive text string that contains from 1 to 22 alphanumeric characters.

For example, to change the hostname to *gssm1.cisco.com*, enter:

```
localhost.localdomain(config)# hostname gssm1.cisco.com
gssm1.cisco.com(config)#
```

To remove the hostname and set it to the default localhost.localdomain, enter:

```
gssm1.cisco.com(config)# no hostname gssm1.cisco.com
localhost.localdomain(config)#
```

Configuring an Ethernet Interface on a GSS Device

Your GSS comes with one integrated dual-port Ethernet controller. This controller provides an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks and supports autonegotitate, full-duplex, or half-duplex operations on an Ethernet LAN.

To configure a GSS Ethernet interface, access global configuration mode and use the **interface ethernet** command. The syntax for this command is as follows:

interface ethernet {**0** | **1**}{**autosense** | **duplex** {**auto** | **full** | **half**} | **gss-communications** | **gss-tcp-keepalives** | **ip address** {*ip-address netmask*} | **no** | **shutdown** | **speed** {*mbits* | **auto**}

If desired, you can use the following CLI commands to configure specific Ethernet interface settings:

- **autosense**
- **duplex** {**auto** | **full** | **half**}
- **gss-communications**
- **gss-tcp-keepalives**
- **ip address** {*ip-address netmask*}
- **shutdown**
- **speed** {*mbits* | **auto**}

The following sections provide detailed information on:

- Configuring an Interface
- Configuring Autosense
- Configuring Interface Duplex Operation
- Configuring Interface Speed
- Configuring GSS Interdevice Communication
- Configuring an Interface for TCP and HTTP HEAD Keepalive Communication
- Setting the IP Address and Subnet Mask of the Ethernet Interface
- Shutting Down an Interface
- Showing Interface Information
- Outputting a Record of TCP Traffic

Configuring an Interface

Use the **interface ethernet** command to configure an Ethernet interface on a GSS device. The syntax for entering an Ethernet interface is as follows:

interface ethernet {**0** | **1**}

The options are:

- **0**—Specifies the first Ethernet interface on a GSS device
- **1**—Specifies the second Ethernet interface on a GSS device

For example, to configure Ethernet interface port 0 on a GSS and access the interface mode, enter:

```
gssm1.cisco.com(config)# interface ethernet 0
```

The GSS changes from configuration mode to the specific interface mode.

```
gssm1.cisco.com(config-eth0)#
```

Configuring Autosense

The **autosense** command enables the current GSS interface to select the proper duplex mode (for example, full duplex, half duplex) for communicating with other network devices. The GSS automatically detects the network line speed (Fast Ethernet only) and duplex of incoming signals, and it synchronizes those parameters during data transfer. Autonegotiation enables the GSS and the other devices on the link to achieve the maximum common level of operation. Autosense is enabled by default.

> ✎
>
> **Note**   You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **autosense** command.

To configure autosense for interface Ethernet 0, enter:

```
gssm1.cisco.com(config)# interface eth0
```

or

```
gssm1.cisco.com(config)# interface eth0
gssm1.cisco.com(config-eth0)# autosense
```

When **autosense** is on, manual configurations are overridden. To prevent your configuration from being overwritten, disable **autosense** before configuring an Ethernet interface.

To disable autosense, use the **no** form of this command. For example, enter:

```
gssm1.cisco.com(config-eth0)# no autosense
```

Configuring Interface Duplex Operation

The **duplex** command enables you to configure an Ethernet interface for full- or half- duplex operation. Full duplex allows data to travel in both directions at the same time through an Ethernet interface. A half-duplex setting ensures that data travels only in one direction at any given time. Although full duplex is faster, the Ethernet interfaces sometimes cannot operate effectively in this mode. If you encounter excessive collisions or network errors, configure the interface for half duplex rather than full duplex. To disable duplex operation, use the **no** form of the command.

Note   You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **duplex** command.

The syntax is as follows:

interface ethernet {0 | 1} duplex {auto | full | half}

The options are:

- **0**—Specifies the first Ethernet interface on a GSS device
- **1**—Specifies the second Ethernet interface on a GSS device
- **auto**—Resets the Fast Ethernet and Gigabit Ethernet ports to automatically negotiate port speed and duplex of incoming signals.
- **full**—Configures an interface for full-duplex operation., which allows data to travel in both directions at the same time.
- **half**—Configures an interface for half-duplex operation, which ensures that data travels in one direction only at any given time.

Note When the GSS 4491 is forced to 1000-Mbps full duplex through the CLI, it goes into autonegotiate mode but operates as specified by advertising only "1000-full." When the GSS 4491 is forced to any other speed or duplex setting, it advertises "forced" rather than "negotiated."

Specify an interface bandwidth (Mbps) using the **speed** command before you configure full- or half-duplex. If you enter the **duplex full or duplex half** command without specifying an interface bandwidth, the following error message appears:

```
Duplex will not be set until speed is set to a non-auto value
```

To configure full duplex for interface Ethernet 0, enter:

```
gssm1.cisco.com(config)# interface eth0 duplex full
```

or

```
gssm1.cisco.com(config)# interface eth0
gssm1.cisco.com(config-eth0)# duplex full
```

To disable duplex operation for interface Ethernet 0, enter:

```
gssm1.cisco.com(config-eth0)# no duplex
```

Configuring Interface Speed

The **speed** option sets the bandwidth on Fast Ethernet interfaces only. Gigabit Ethernet interfaces run at 1000 Mbps only and are not user-configurable. To restore default values, use the **no** form of this command.

Note You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **speed** command.

The syntax is:

interface ethernet {**0** | **1**} **speed** *mbits*

Specify the bandwidth size in megabits per second (Mbps). The default speed for a GSS interface is autonegotiate. The available ranges are as follows:

- **10**—Initiates 10-Mbps operation
- **100**—Initiates 100-Mbps operation
- **1000**—Initiates 1000-Mbps operation
- **auto**—Enables the GSS to autonegotiate with other devices (default)

Note The interface speed of the GSS 4490 cannot be configured to 1000-Mbps by using the **interface ethernet** {**0** | **1**} **speed** command. If you attempt to specify an operating speed of 1000, the GSS 4490 remains set at the previous setting (as displayed through the **show interface** command). To enable a GSS 4490 interface to operate at 1000 Mbps, specify **auto**. The autonegotiate selection allows the GSS 4490 autonegotiate to 1000 Mbps with other devices.

To set the bandwidth on Ethernet 0, enter:

```
gssm1.cisco.com(config)# interface eth0 speed 100
```

or

```
gssm1.cisco.com(config)# interface eth0
gssm1.cisco.com(config-eth0)# speed 100
```

To restore the default setting of autonegotiate for interface Ethernet 0, enter:

```
gssm1.cisco.com(config-eth0)# no speed
```

Configuring GSS Interdevice Communication

During inter-GSS communication, all GSS devices listen for configuration and status updates on only one interface. The default inter-GSS communication interface is Ethernet 0. To designate Ethernet interface 1 for inter-GSS communication, use the **gss-communications** option.

> ✎
>
> **Note** You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **gss-communications** command.

To designate Ethernet 1 for GSS interdevice communication, enter:

```
gssm1.cisco.com(config)# interface eth1 gss-communications
```

or

```
gssm1.cisco.com(config)# interface eth1
gssm1.cisco.com(config-eth1)# gss-communications
```

Configuring an Interface for TCP and HTTP HEAD Keepalive Communication

To designate one of the two GSS Ethernet interface s as the source for TCP and HTTP HEAD keepalive communication, use the **gss-tcp-keepalives** option. Only one Ethernet interface (0 or 1) can be designated for TCP and HTTP HEAD keepalive communication.

Note You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **gss-tcp-keepalives** command.

For example, to designate Ethernet 1 for TCP and HTTP HEAD keepalive communication, enter:

```
gssm1.cisco.com(config)# interface eth1 gss-tcp-keepalives
```

or

```
gssm1.cisco.com(config)# interface eth1
gssm1.cisco.com(config-eth1)# gss-tcp-keepalives
```

Setting the IP Address and Subnet Mask of the Ethernet Interface

Use the **ip address** command to assign an IP address and subnet mask to an Ethernet interface. You cannot assign the same IP address to more than one interface. To disable a specific IP address, use the **no** form of the command.

The syntax is:

> **ip address** *ip-address ip-subnet*

The variables are:

- *ip-address*—IP address of the Ethernet interface. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

- *ip-subnet*—Subnet mask of the interface. The subnet mask of the interface in dotted-decimal notation (for example, 255.255.255.0).

Note You cannot enter interface commands while the GSS software is running (for example, serving DNS requests). Enter the **gss stop** command to stop the GSS software before executing the **ip address** command.

To assign an IP address to Ethernet 0, enter:

```
gssm1.cisco.com(config)# interface eth0 ip address 192.168.10.2
255.255.255.0
```

or

```
gssm1.cisco.com(config)# interface eth0
gssm1.cisco.com(config-eth0)# ip address 192.168.10.2 255.255.255.0
```

To remove an IP address and subnet mask for interface Ethernet 0, enter:

```
gssm1.cisco.com(config)# interface eth0
gssm1.cisco.com(config-eth0)# no ip address
```

Shutting Down an Interface

Use the **shutdown** command in interface configuration mode to shut down a particular Ethernet interface on the GSS device.

To shut down interface Ethernet 1, enter:

```
gssm1.cisco.com(config)# interface eth1 shutdown
```

or

```
gssm1.cisco.com(config)# interface eth1
gssm1.cisco.com(config-eth1)# shutdown
```

Showing Interface Information

To display GSS hardware interface information for Ethernet interface 0 or 1, including interface statistics, use the **show interface** command.

> **show interface** {**eth0** | **eth1**}

For example, to display information for Ethernet interface 0, enter:

```
gssm1.cisco.com# show interface eth0
Interface eth0
   ip address 10.86.209.167 255.255.254.0
   gss-communications

Interface State
   Link is up
   negotiated, 100 mbps, full duplex
   Supported modes:  10-half, 10-full, 100-half, 100-full, 1000-full
   Advertised modes: 10-half, 10-full, 100-half, 100-full, 1000-full

Interface statistics
   eth0      Link encap:Ethernet  HWaddr 00:C0:9F:35:D1:64
             inet addr:10.86.209.167  Bcast:10.86.209.255
Mask:255.255.254.0
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:583003 errors:0 dropped:0 overruns:0 frame:0
             TX packets:114048 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:45735671 (43.6 Mb)  TX bytes:9810113 (9.3 Mb)
             Base address:0xbc00 Memory:fc9e0000-fca00000
```

Outputting a Record of TCP Traffic

Use the **tcpdump interface** command to display a record at the CLI of all TCP traffic transmitted from and received by an Ethernet interface. GSS traffic information continuously displays on screen until you press **Ctrl-C** to cancel the operation. The **protocol**, **port**, **network**, and **file** options of the **tcpdump** command allow you to filter traffic and capture only the traffic of certain protocols, going to or coming from certain hosts or certain ports.

The syntax for this command is as follows:

> **tcpdump interface** {**any** | **eth0** | **eth1**} | **protocol** {**any**| **icmp**|**tcp**|**udp**} | **host** {**any** | *ip_or_host*} | **port** {**any** | *port*} | **network** {**any** | *ip-address ip-subnet*} | **file** {*filename*}

The keywords and arguments are as follows:

- **any**—Instructs the GSS software to accept all selections for an associated option. For example, if you enter **tcpdump interface any any**, the GSS filters the ICMP, TCP, and UDP IP protocols on Ethernet 0 and 1.

- **eth0**—Outputs a record of all traffic transmitted from and received by interface Ethernet 0.

- **eth1**—Outputs a record of all traffic transmitted from and received by Ethernet 1.

- **protocol** {**icmp**|**tcp**|**udp**}—Filters the protocol for the traffic type. Recognized IP protocols include:

    - **icmp**—Internet Control Message Protocol

    - **tcp**—Transmission Control Protocol

    - **udp**—User Datagram Protocol

- **host** {*ip_or_host*}—Filters the host machine that is the source or destination of the packet. The software uses the IP address or hostname of the device that is the source or destination of the packet.

- **port** {*port*}—Filters the source or destination port of the packet.

- **network** {*ip-address ip-subnet*}—Filters the network IP address from which the packet originated. The software uses the *ip-address* and *ip-subnet* arguments to match the incoming packet to a source network.

- **file** {*filename*}—Enables you to capture raw data to a file. Then you can open the captured raw data in a Sniffer tool. When capturing data to a file, the entire packet is captured. A maximum of 20,000 filtered packets can be captured to disk. This packet limit is meant to prevent you from accidentally filling up the disk when capturing data using the **tcpdump** command.

    If the file parameter is not specified, captured data is dumped to the screen. In that case, only header data is displayed and there is no limit to number of packets captured.

If you execute the **tcpdump** command without any specified options, no filtering is performed. If you want to use the defaults for the remaining **tcpdump** command parameters, press **Enter** at each option. No further filtering is performed by the GSS, other than what has been specified. For example, if you enter `tcpdump interface eth0 protocol tcp`, the GSS performs only IP protocol filtering and does not perform host, port, or network filtering.

The following is an example of the **tcpdump interface** command and its output:

```
gssm1.cisco.com# tcpdump interface eth0
Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on eth0
19:20:45.678641 > gssm.cisco.com.ssh > 10.1.2.3.1178: P
2126255246:2126255346(100) ack 4828790 win 32680 (DF) [tos 0x10]
19:20:45.680534 > gssm.cisco.com.49165 > gss.cisco.com.domain: 9217+
PTR? 187.0.1.2.in-addr.arpa. (43)
19:20:45.681090 < gss.cisco.com.domain > gssm.cisco.com.49165: 9217
NXDomain* 0/1/0 (111)
...
```

Specifying Name Servers

The GSS can communicate with a maximum of eight name servers for name and address resolution. Use the **ip name server** command to specify the IP address of one or more name servers, to a maximum of eight name servers. To disable one or more name servers, use the **no** form of this command.

The syntax for this command is as follows:

> **ip name-server** *ip-addresses*

The ip-addresses variable identifies the IP addresses for the name servers. You can enter a maximum of eight name servers, separated by spaces. Enter each IP address in dotted-decimal notation.

To configure the IP address of a single name server, enter:

```
gssm1.cisco.com(config)# ip name-server 172.16.17.18
```

To configure the IP addresses of multiple name servers, enter:

```
gssm1.cisco.com(config)# ip name-server 172.16.17.18 192.168.2.22
172.16.1.2
```

The GSS requires a functioning nameserver to operate properly and perform DNS resolutions. If the nameserver is not properly configured using the **ip name-server** command, or if the configured nameservers are not reachable for any reason (down, network loss, or a firewall), the GSS will not be able to perform DNS resolutions when you attempt to log in. In this case, the timeout may take several minutes. This behavior occurs when you attempt to log in through a Telnet, SSH, or FTP connection.

To enable the GSS to perform DNS resolution, always configure more than one nameserver. For example:

```
gss.example.com(config)#ip name-server 192.168.1.1
gss.example.com(config)#ip name-server 192.168.2.2
gss.example.com(config)#ip name-server 192.168.3.3
```

This behavior may also occur if you configure access lists for the GSS. In this case, create access lists that allow the DNS responses from a nameserver. For example:

```
gss.example.com(config)#access-list acl1 permit udp any eq 53
```

Another solution is to limit incoming DNS response packets only from your configured nameservers (more secure). For example:

```
gss.example.com(config)#access-list acl1 permit udp 192.168.1.1
255.255.255.255 eq 53
gss.example.com(config)#access-list acl2 permit udp 192.168.1.2
255.255.255.255 eq 53
gss.example.com(config)#access-list acl3 permit udp 192.168.1.3
255.255.255.255 eq 53
```

Configuring an IP Route for the GSS

To establish IP connectivity to the GSS, configure a static IP route to connect the GSS to next hop router. A static route consists of a destination network address and mask and the next hop to reach the destination. You can also specify a default static route (using 0.0.0.0 as the destination network address and a valid next hop address) to direct IP packets for which no other destination is listed in the routing table. Default static routes are useful for forwarding otherwise unrouteable packets by the GSS.

Use the following **ip** command options to configure a static IP route:

- **ip default-gateway**—Defines a default gateway. To delete the IP default gateway, use the **no** form of this command. The GSS uses the default gateway to route IP packets when there is no specific route found to the destination.

- **ip route**— Adds a specific static route for a network host. Any IP packet designated for the specified host uses the configured route. To disable an IP routing, use the **no** form of this command.

The syntax for the **ip** command is:

> **ip** {**default-gateway** *ip-address* | **route** *destination_address netmask gateway*}

> **no ip** {**default-gateway** *ip-address* | **route** *destination_address netmask gateway*}

The keywords and arguments are as follows:

- **default-gateway**—Specifies the default gateway (if not routing IP).
- *ip-address*—Specifies an IP address for the default gateway. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- **route**—Specifies the network route.
- *destination_address*—Specifies the destination IP route address. Enter the IP address in dotted-decimal notation.
- *netmask*—Specifies the subnet mask. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- *gateway*—Specifies the gateway IP address. Enter the IP address in dotted-decimal notation.

For example, to configure a default gateway, enter:

```
gssm1.cisco.com(config)# ip default-gateway 192.168.7.18
```

For example, to configure a static IP network route, enter:

```
gssm1.cisco.com(config)# ip route 172.16.227.128 172.16.227.250
```

To display the IP routing table for the GSS, use the **show ip routes** command.

```
gssm1.cisco.com# show ip routes
```

Table 4-4 describes the fields in the **show ip routes** output.

Table 4-4   Field Descriptions for show ip routes Command

Field	Description
User Defined Routes	Static IP routes configured for the GSS.
Kernel IP Routing Table	IP routing information for the GSS.
Destination	Destination network or destination host.
Gateway	Gateway address (or 0.0.0.0 if no gateway address is set).

Table 4-4   Field Descriptions for show ip routes Command (continued)

Field	Description
Genmask	Subnet mask for the destination network.
Flags	Possible flags are as follows: • U (route is up) • H (target is a host) • G (use gateway) • R (reinstate route for dynamic routing) • D (dynamically installed by daemon or redirect) • M (modified from routing daemon or redirect) • A (installed by addrconf) • C (cache entry) • ! (reject route)
Metric	Distance to the target, usually counted in hops.
Ref	Number of references to this route.
Use	Count of lookups for the route.
Iface	Interface to which packets for this route will be sent.

Resolving a Host or Domain Name to an IP Address

To resolve a host or domain name to an IP address, use the **dnslookup** command. The syntax for this command is as follows:

> **dnslookup** {*hostname* | *domainname*}

The variables are:

• *hostname*—Name of the host on the network.

• *domainname*—Name of the domain.

In the example, the **dnslookup** command resolves the hostname **myhost.cisco.com** to IP address 172.16.69.11.

```
gssm1.cisco.com# dnslookup myhost.cisco.com
Server:  mydnsserver.cisco.com
Address:  172.16.69.12

Name:    myhost.cisco.com
Address: 172.16.69.11
```

Configuring a Primary GSSM

The primary GSSM performs content routing as well as centralized management functions for the GSS network. The primary GSSM serves as the organizing point of the GSS network, hosting the embedded GSS database that contains configuration information for all of your GSS resources, such as individual GSS devices and DNS rules. Other GSS devices report their status to the primary GSSM. The primary GSSM offers a single, centralized GUI for monitoring and administering your entire GSS network.

A typical GSS deployment may contain a maximum of eight GSS devices on a corporate intranet or the Internet. At least one GSS—and no more than two GSS devices—must be configured as the primary GSSM and standby GSSM. The primary GSSM monitors the other GSS devices on the network and offers features for managing and monitoring request routing services using a GUI accessible through secure HTTP. Only one primary GSSM can be "active" at any time, with the second GSSM serving as a "standby," or backup device.

Before you configure request routing or add GSS devices to your GSS network, first configure and enable a primary GSSM. After you have configured a primary GSSM, you may optionally configure a different GSS as the standby (redundant) GSSM.

Use the **gss enable gssm-primary** command to create the embedded database on the primary GSSM. This command also performs the other initialization processes to enable the device in a network of GSS devices. Enabling a GSS device is a one-time initialization step that is required only when you first set up the device within a network of GSS devices.

To configure a GSS device as a primary GSSM, perform the following steps:

1. Log in to the CLI of the GSS device and enable privileged EXEC mode. GSS configuration requires that you enter into privileged EXEC mode on the CLI. Ensure that your login has adequate permissions.

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

2. Enter the **gss enable gssm-primary** command to configure your GSS device as the primary GSSM in the GSS network.

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

✎

Note   When you use the **gss enable gssm-primary** command and a database exists on this GSS device, an error message appears. If this error message appears, use the **gss disable** command to remove the existing configuration and return the GSS device to its initial state, which includes deleting the GSSM database from the GSS device.

3. Save your configuration changes to memory.

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

If you fail to save your configuration changes, the GSS device reverts to its previous settings upon a reboot.

At this point, you can access the GUI on the primary GSSM. After logging in to the primary GSSM GUI, use it to activate the standby GSSM and GSS devices on your network, as described in Chapter 5, Activating GSS Devices from the GUI.

Configuring a Standby GSSM

The standby GSSM performs GSLB functions for the GSS network even while operating in standby mode. In addition, the standby GSSM can be configured to act as the GSSM should the primary GSSM need to go offline for repair or maintenance, or becomes unavailable to communicate with other GSS devices. As with the primary GSSM, the standby GSSM is configured to run the GSSM GUI and contains a duplicate copy of the embedded GSS database that is currently installed on the primary GSSM. Any configuration or network changes affecting the GSS network are synchronized between the primary and the standby 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. For details about changing the GSSM role in your GSS network, see the *Cisco Global Site Selector Administration Guide*, Chapter 1, Managing GSS Devices from the GUI.

To configure a GSS device as a standby GSSM, perform the following steps:

1. If you have not done so already, configure and enable a primary GSSM as described in the "Configuring a Primary GSSM" section.

2. Log in to the CLI of the GSS device and enable privileged EXEC mode. GSS configuration requires that you enter into privileged EXEC mode on the CLI. Ensure that your login has adequate permissions to do so.

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

3. Enter the **gss enable gssm-standby** command to enable your standby GSSM device and direct it to the primary GSSM in your GSS network. This command registers the standby GSSM with the primary GSSM.

The syntax for this command is as follows:

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

The variables are:

– *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 gss2.example.com as the standby GSSM and direct it to the primary GSSM, gssm1.example.com, enter:

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

4. Save your configuration changes to memory.

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

If you fail to save your configuration changes, the GSS device reverts to its previous settings upon a reboot.

Configuring a Global Site Selector

The GSS performs routing of DNS queries based on DNS rules and conditions configured using the primary GSSM. Each GSS is known to and synchronized with the GSSM, but individual GSS devices do not report their presence or status to the other. Each GSS on your network delegates authority to the GSS devices that serve DNS requests. Each GSS is managed separately using the Cisco CLI. GUI support is not available on a GSS device.

To configure a GSS device, perform the following steps:

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

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

✎

Note   GSS configuration requires that you enter into privileged EXEC mode on the CLI. Ensure that your login has adequate permissions to do so.

2. Use the **gss enable** command to enable your GSS device as a GSS and direct it to the primary GSSM in your GSS network. Specify either the domain name or the network address of the primary GSSM.

The syntax for this command is as follows:

gss enable gss *primary_GSSM_hostname | primary_GSSM_IP_address*

The variables are:

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

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

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

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

3. Save your configuration changes to memory.

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

If you fail to save your configuration changes, the device reverts to its previous settings upon a reboot.

Where to Go Next

To activate and register your standby GSSM and GSS devices from the primary GSSM GUI, proceed to Chapter 5, Activating GSS Devices from the GUI. This chapter also describes how to log in to the primary GSSM GUI.

You can also activate and configure your GSS devices from the CLI instead. To do so, proceed to Chapter 6, Activating GSS Devices from the CLI.

Activating GSS Devices from the GUI

This chapter describes how to log on to the primary GSSM and active your GSSM and GSS devices from the primary GSSM GUI as the first step in configuring request routing and global server load balancing on your GSS network.

This chapter contains the following major sections:

- Logging In to the Primary GSSM Graphical User Interface
- Activating GSS Devices from the Primary GSSM
- Where to Go Next

Logging In to the Primary GSSM Graphical User Interface

After you configure and enable your primary GSSM, you may access the graphical user interface (GUI). The primary GSSM uses HTTP over SSL (HTTPS) to communicate with web clients.

When you first log in to the primary GSSM GUI, use the system default administrative account and password. After you access the primary GSSM GUI, create and maintain additional user accounts and passwords using the user administration features of the primary GSSM. See the *Cisco Global Site Selector Administration Guide* for information on creating user accounts.

To log in to the primary GSSM GUI, perform the following steps:

1. Open your preferred Internet web browser application, such as Internet Explorer or Netscape Navigator.

2. Enter the secure HTTP address of your GSSM in the address field. For example, if your primary GSSM is named gssm1.example.com, enter the following to display the primary GSSM login dialog box and to access the GUI:

   https://gssm1.example.com

   If you have trouble locating the primary GSSM DNS name, keep in mind that the GSS network uses secure connections. The address of the GSSM includes https:// (HTTP over SSL) instead of the more common http://.

3. Click **Yes** at the prompt to accept (trust) and install the signed certificate from Cisco Systems.

   To avoid approving the signed certificate every time you log in to the primary GSSM, accept the certificate from Cisco Systems, Inc. For instructions on trusting certificates from a particular owner or website, see the online help included with your browser.

4. To install the signed certificate, if you are using one of the following:

   – Internet Explorer—In the Security Alert dialog box, click **View Certificate**, choose the **Install Certificate** option, and follow the prompts of the Certificate Manager Import Wizard. Proceed to Step 5.

   – Netscape—In the New Site Certificate dialog box, click **Next** and follow the prompts of the New Site Certificate Wizard. Proceed to Step 5.

5. At the primary GSSM login window, enter your username and password in the fields provided, and then click **Login** (see Figure 5-1). If this is your first time logging on to the GSSM, use the default account name (admin) and password (default) to access the GUI.

   The Primary GSSM Welcome page (see Figure 5-2) appears. See the *Cisco Global Site Selector GUI-based Global Server Load-Balancing Configuration Guide* for information on navigating through the primary GSSM GUI.

Figure 5-1   Primary GSSM GUI Login Window
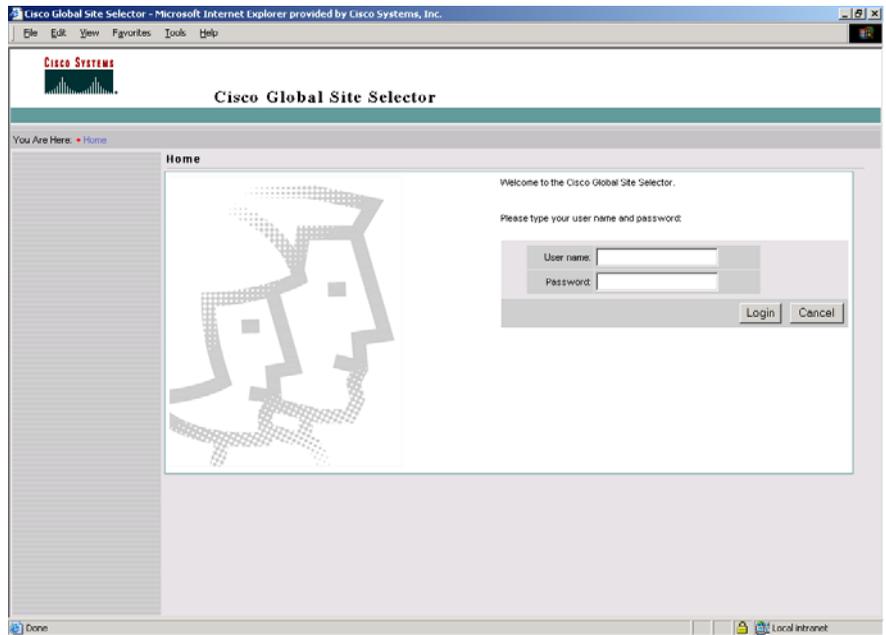
Figure 5-2   Primary GSSM Welcome Window
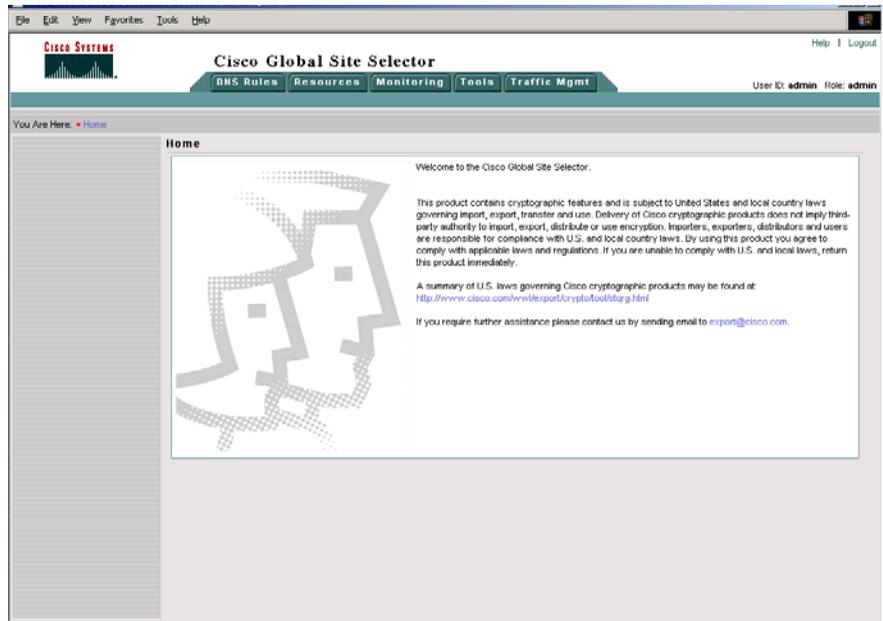
To log out of a primary GSSM GUI session, click **Logout** at the upper right of the window. The browser confirms that you want to log out of the primary GSSM GUI session. Click **OK** to confirm the logout (or **Cancel**). When you click **OK**, the primary GSSM logs you out of the session and redisplays the Primary GSSM GUI Login window (see Figure 5-1).

Activating GSS Devices from the Primary GSSM

After you configure your GSS devices to function as a standby GSSM or as a GSS, activate those devices from the primary GSSM GUI to add those devices to your GSS network. The standby GSSM and GSS devices are synchronized with the primary GSSM.

To activate a GSS or a standby GSSM from the primary GSSM GUI, perform the following steps:

1. Click the **Resources** tab.

2. Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears (see Figure 5-3). All active GSS devices appear with an "Online" status. The GSS devices requiring activation appear with an "Inactive" status.

Figure 5-3   Global Site Selectors List Page—Inactive Status
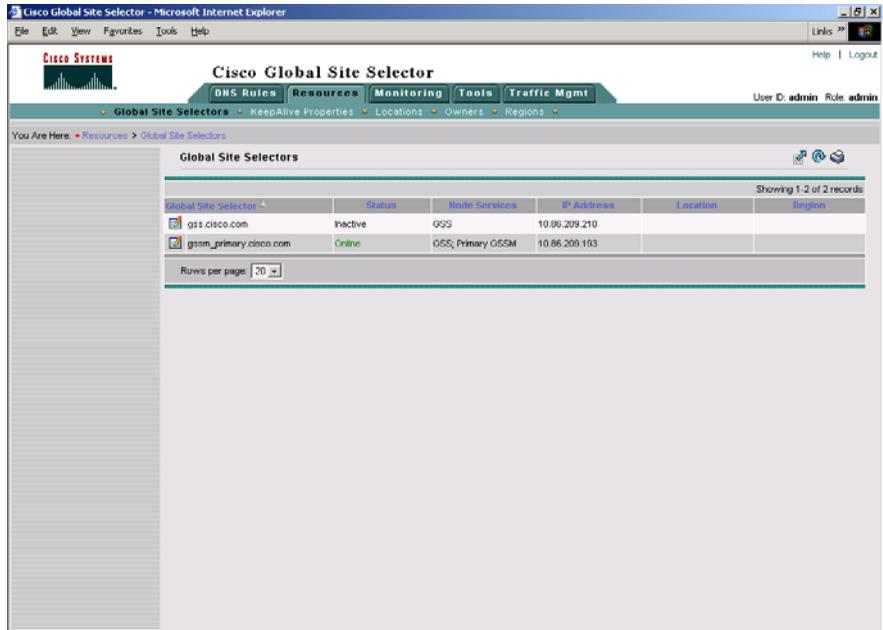
3. Click the **Modify GSS** icon for the first GSS device to activate. The Modifying GSS details page appears (see Figure 5-4).

Figure 5-4   Modifying GSS Details Page

4. Check the **Activate** check box. This check box does not appear in the Modifying GSS details page until after a GSS device has been activated.

5. Click the **Submit** button, which returns you to the Global Site Selectors list page (see Figure 5-5). The status of the active GSS device is "Online." If the device is functioning properly and network connectivity is good between the device and the primary GSSM, the status of the device changes to "Online" within approximately 30 seconds.

✎

Note   The device status remains "Inactive" if the device is not functioning properly or there are problems with network connectivity. If this situation occurs, cycle power to the GSS device, check your network connections, then repeat this procedure. If you still cannot activate the GSS device, contact Cisco TAC.

Figure 5-5   Global Site Selectors List Page—Active Status
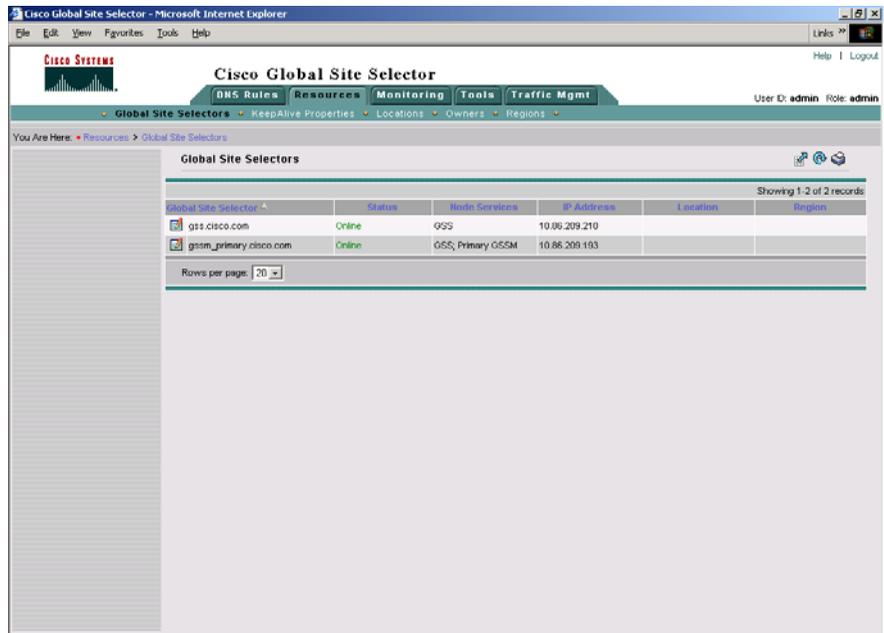
6. Repeat Steps 1 through 5 for the standby GSSM and each inactive GSS device.

Where to Go Next

After you create your GSSM (primary and standby) and GSS devices and configure them to connect to your network, you can begin configuring request routing and global server load balancing on your GSS network. To configure your GSS devices and resources from the primary GSSM for global server load-balancing, proceed to Chapter 7, Global Server Load Balancing Summary.

C H A P T E R **6**

Activating GSS Devices from the CLI

This chapter describes how to activate GSS devices from the primary GSSM CLI as the first step in configuring request routing and global server load balancing on your GSS network.

This chapter contains the following major sections:

- Activating or Deleting GSS Devices from the Primary GSSM
- Displaying the Configuration for Registered GSS Devices
- Using Scripts in GSLB Configuration
- Where to Go Next

Activating or Deleting GSS Devices from the Primary GSSM

After you log in to the CLI and enable privileged EXEC mode, you enter the **gslb** command to access the global server load-balancing configuration mode. The CLI prompt then changes to (config-gslb). For example:

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

To activate the registered GSS devices on the primary GSSM, perform the following steps:

1. Modify or activate GSS device configuration by using the **gss-device** command. Specifically, this command does the following:

   – Activates the GSS device

   – Changes the Location

   – Changes the Name

The syntax for this command is as follows:

gss-device *Name* [**name** *newName*] [**location** *locationName*] **activate**

The keywords and arguments are as follows:

   – *name*—Specifies the GSS device name.

   – **name** *newName*—(Optional) Specifies the new GSS device name.

   – **location** *locationName*—(Optional) Specifies the GSS location. The
     location is part of the overall GSLB configuration

   – **activate**—Activates the specified GSS. Be aware that you can only
     activate one GSS at a time.

For example:

```
gss1.com(config-gslb)# gss-device gss-sample.cisco.com name name1
location sj activate
gss1.com(config-gslb)#
```

If the named GSS is not registered, the command displays an error message.

Note   The configuration for this command is stored in the GSLB configuration and
propagated to the other GSS devices in the mesh.

   2. Delete a GSS device by using the **no gss-device** command. The syntax for this
       command is as follows:

no gss-device *Name*

The *name* argument specifies the GSS that you wish to delete.

If there is no GSS with the specified name, an error message appears.

Note   The **no gss-device** command clears the device status from the **show gslb-config
gss-device** command output. For more information on this command, see the
"Displaying the Configuration for Registered GSS Devices" section.

3. Clear the GSLB configuration from the **show gslb-config gss-device** command output by using the **clear gslb-config** command.

The syntax for this command is as follows:

clear gslb-config

For example:

```
gss1.com# clear gslb-config
gss1.com#
```

If a location is referenced in the GSS configuration, the location and region fields are cleared from the configuration by this command.

✎
Note   If you attempt to delete a location while it is being used in the GSS configuration, an error message displays and the command is not executed.

Displaying the Configuration for Registered GSS Devices

To display configuration information for registered GSS devices, perform the following steps:

1. List all the registered GSS devices and display minimal information for each by using the **show resources gss-device** command. The syntax for this command is as follows:

show resources gss-devices

For example:

```
gss-kingfisher.cisco.com#show resources gss-device
GSS Device: gss-kingfisher.cisco.com
    Status : Online
    Node Services: GSS; Primary GSSM
    IP Address: 16.1.1.105
    Location   : Bangalore
    Region : India

GSS Device: gss-kiwi.cisco.com
    Status : Online
    Node Services: GSS
```

```
                        IP Address: 16.1.1.114
                        Location   : SJ
                        Region  : USA
```

2. Display complete information for a specified device by using the **show resources gss-device** command followed by a given name.

   The syntax for this command is as follows:

   show resources gss-devices *name*

   For example:

```
gss-kingfisher.cisco.com#show resources gss-device

GSS Device: gss-kingfisher.cisco.com

    General Configuration
        Name    : gss-kingfisher.cisco.com

    Locality
        Location   : Bangalore
        Region  : India

    Node Information
        Status  : Online
        Version    : 2.0.0.0.5
        Node Services: GSS; Primary GSSM

    Network Information
        IP Address : 16.1.1.105
        HostName   : gss-kingfisher.cisco.com
        Mac        : 00:c0:9f:e4:12:ef
```

3. List only the devices which are activated from the GUI or CLI among the registered devices by using the **show gslb-config gss-device** command.

   The syntax for this command is as follows:

   show gslb-config gss-device

   For example:

```
gss-kingfisher.cisco.com#show gslb-config gss-device
gss-device gss-kingfisher.cisco.com location Bangalore activate
```

Using Scripts in GSLB Configuration

If you wish, you can copy and use scripts in GSLB configuration using the **script play-config** command.

The syntax for this command is as follows:

script play-config *filename*

The f*ilename* variable is the name of a previously created GSLB configuration file that resides on the root directory of the primary GSSM. The GSLB configuration file could be a file that was created on the primary GSSM on which it resides, or it could be a file that was created on the primary GSSM on another GSS network, then copied to this primary GSSM.

For example, if you take a GSS configuration from the primary GSSM A using the following CLI command:

copy gslb-config disk *filename*

You can then execute this configuration on primary GSSM B by using **script play-config** as follows:

```
gss1.com(config-gslb)# script play-config sampleconfig
gss1.com(config-gslb)#
```

This command will then run the commands to activate the device on the primary GSSM B if the device is registered with the same name. For more information on executing GSLB configuration files using **script play-config**, see the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide.*

Note   When upgrading from pre-v2.0 versions of the GSS software to v2.0, the entire registered GSS device configuration is retained.

Where to Go Next

After you activate your GSS devices from the primary GSSM, you can begin configuring request routing and global server load balancing on your GSS network. To configure your GSS devices and resources from the primary GSSM for global server load-balancing, proceed to Chapter 7, , Global Server Load Balancing Summary.

C H A P T E R 7

Global Server Load Balancing Summary

After you create your GSSM (primary and standby) and GSS devices and configure them to connect to your network, you can begin to configure request routing and global server load balancing on your GSS network. When you perform GSLB configuration and monitoring for your GSS network, in most cases you have the option of using either the centralized GUI or CLI on the primary GSSM.

For tasks that you can perform using either the CLI or the GUI of the primary GSSM, choosing when to use the CLI or the GUI is a matter of personal or organizational choice. However, not every GSLB configuration and monitoring task is available from the GUI and the CLI of the primary GSSM. A few examples are as follows:

- You configure sticky and proximity groups using the CLI of the primary GSSM

- You create DNS view filters using the GUI of the primary GSSM

- You perform sticky database and proximity database management using the CLI of each GSS device.

For an overview of different global server load-balancing configuration tasks that you can perform from either the primary GSSM GUI or CLI, from only the primary GSSM GUI, or from only the primary GSSM CLI, see Table 1-2 in Chapter 1, Using the CLI and GUI to Manage a GSS Network.

See either the *Cisco Global Site Selector GUI-based Global Server Load-Balancing Configuration Guide* or the *Cisco Global Site Selector CLI-based Global Server Load-Balancing Configuration Guide* for detailed procedures on how to configure your GSS devices to perform global server load balancing.

Use the following procedures to configure your GSS devices and resources from the primary GSSM for global server load balancing:

1. Create regions, locations, and owners—Optional. Use these groupings to organize your GSS network resources by customer account, physical location, owner, or other organizing principle. See Chapter 2, Configuring Resources, for details.

2. Create one or more source address lists—Optional. Use these lists of IP addresses to identify the name servers (D-proxy) that forward requests for the specified domains. The default source address list is Anywhere to match any incoming DNS request to the domains. See Chapter 3, Configuring Source Address Lists, for details.

3. Create one or more domain lists—Establish lists of Internet domains, possibly using wildcards, that are managed by the GSS and queried by users. See Chapter 4, Configuring Domain Lists, for details.

4. Modify the default global keepalive settings or create any shared keepalives—Optional. These are GSS network resources that are regularly polled to monitor the online status of one or more GSS resources linked to the keepalive. Shared keepalives are required for any answer that uses the KAL-AP keepalive type. See Chapter 5, Configuring KeepAlives, for details.

5. Create one or more answers and answer groups—Answers are resources that match requests to domains. Answer groups are collections of resources that balance requests for content. See Chapter 6, Configuring Answers and Answer Groups, for details.

6. Build the DNS rules that will control global server load balancing on your GSS network. See Chapter 7, Building and Modifying DNS Rules for details.

7. If you plan to use DNS sticky for your global server load-balancing application, configure local and global DNS sticky for GSS devices in your network—Stickiness enables the GSS to remember the DNS response returned for a client D-proxy and to later return that answer when the client makes the same request. See Chapter 8, Configuring DNS Sticky, for details.

8. If you plan to use network proximity for your global server load-balancing application, configure proximity for GSS devices in your network—Proximity determines the best (most proximate) resource for handling global load-balancing requests. See Chapter 9, Configuring Network Proximity, for details.

I N D E X