



Cisco Global Site Selector Getting Started Guide

Software Version 1.3
March 2006

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8942-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

Cisco Global Site Selector Getting Started Guide

Copyright © 2006 Cisco Systems, Inc. All rights reserved.



Preface	xi	
Audience	xii	
How to Use This Guide	xiii	
Related Documentation	xiv	
Symbols and Conventions	xvi	
Obtaining Documentation	xviii	
Cisco.com	xviii	
Product Documentation DVD	xviii	
Ordering Documentation	xix	
Documentation Feedback	xix	
Cisco Product Security Overview	xx	
Reporting Security Problems in Cisco Products	xx	
Obtaining Technical Assistance	xxi	
Cisco Technical Support & Documentation Website	xxi	
Submitting a Service Request	xxii	
Definitions of Service Request Severity	xxiii	
Obtaining Additional Publications and Information	xxiii	
CHAPTER 1	Using the CLI and GUI to Manage a GSS Network	1-1
	CLI and GUI Network Management Overview	1-2
	Summary of Tasks Using the CLI and the GUI	1-3
CHAPTER 2	Configuring the GSS Using the CLI Setup Script	2-1
	Using the Setup Script	2-1

Where to Go Next 2-5

CHAPTER 3

Accessing the GSS CLI 3-1

Accessing the CLI Using a Direct Serial Connection 3-1

Logging in to the CLI and Enabling Privileged EXEC Mode 3-3

Remotely Accessing a GSS Device 3-3

 Enabling Remote Access on a GSS Device 3-4

 Accessing the CLI Using a Remote Connection 3-7

 Accessing the CLI Over SSH Using a Private and Public Key Pair 3-7

Where to Go Next 3-9

CHAPTER 4

Setting Up Your GSS from the CLI 3-1

Initial Setup Quick Start 3-2

Logging in to the CLI and Enabling Privileged EXEC Mode 3-5

Setting the System Clock 3-6

 Setting the Time and Date 3-6

 Setting the Time Zone 3-7

 Setting the Hardware Clock 3-8

 Synchronizing the GSS System Clock with an NTP Server 3-9

 Showing the Date, Time, and Timezone 3-10

Configuring a Host Name for the GSS Device 3-11

Configuring an Ethernet Interface on a GSS Device 3-12

 Configuring an Interface 3-13

 Configuring Autosense 3-13

 Configuring Interface Duplex Operation 3-14

 Configuring Interface Speed 3-16

 Configuring GSS Inter-Device Communication 3-17

 Configuring an Interface for TCP and HTTP HEAD Keepalive
Communication 3-17

Setting the IP Address and Subnet Mask of the Ethernet Interface	3-18
Shutting Down an Interface	3-19
Showing Interface Information	3-19
Outputting a Record of TCP Traffic	3-20
Specifying Name Servers	3-22
Configuring an IP Route for the GSS	3-23
Resolving a Host or Domain Name to an IP Address	3-25
Configuring a Primary GSSM	3-26
Configuring a Standby GSSM	3-27
Configuring a Global Site Selector	3-29
Where to Go Next	3-30

CHAPTER 5**Activating GSS Devices from the GUI** 5-1

Logging In to the Primary GSSM Graphical User Interface	5-1
Activating GSS Devices from the Primary GSSM	5-4
Where to Go Next	5-7

CHAPTER 6**Global Server Load Balancing Summary** 6-1

INDEX



<i>Figure 5-1</i>	Primary GSSM GUI Login Window	5-3
<i>Figure 5-2</i>	Primary GSSM Welcome Window	5-4
<i>Figure 5-3</i>	Global Site Selectors List Page—Inactive Status	5-5
<i>Figure 5-4</i>	Modifying GSS Details Page	5-6
<i>Figure 5-5</i>	Global Site Selectors List Page—Active Status	5-7



TABLES

<i>Table 1-1</i>	Using the CLI or GUI to Perform Configuration Tasks	1-3
<i>Table 1-2</i>	Using the CLI or GUI to Perform GSLB Configuration Tasks	1-5
<i>Table 4-1</i>	Initial Setup Quick Start	3-2
<i>Table 4-2</i>	Field Descriptions for the show clock Command	3-10
<i>Table 4-3</i>	Field Descriptions for show ip routes Command	3-24



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 describes the following topics:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

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 your organization's specific network configuration.

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, 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
<i>Global Site Selector Hardware Installation Guide</i>	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.
<i>Regulatory Compliance and Safety Information for the Cisco Global Site Selector</i>	Regulatory compliance and safety information for the GSS.
<i>Release Note for the Cisco Global Site Selector</i>	Information on operating considerations, caveats, and new CLI commands for the GSS software.
<i>Cisco Global Site Selector Administration Guide</i>	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.
<i>Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide</i>	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
<i>Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide</i>	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.
<i>Cisco Global Site Selector Command Reference</i>	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 .
<i>italic font</i>	Variables for which you supply values are in <i>italics</i> .
[]	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 <i>screen font</i> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Variables for which you supply values are in <i>italic screen font</i> .
→	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.
<code>Courier text</code>	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.
<i>italic text</i>	Directories and filenames are in <i>italic</i> 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



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 provides you with an overview on 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 summarizes when to use:

- 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 major 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:

- 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.

Proceed to the [“Summary of Tasks Using the CLI and the GUI”](#) section for a detailed overview on 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. The 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				Related Document	
	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	<i>Cisco Global Site Selector Getting Started Guide Chapter</i>	<i>Cisco Global Site Selector Administration Guide</i>
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	—	—	Yes	Chapter 5, Activating GSS Devices from the GUI	—
Delete GSS devices from the GSS network	—	—	Yes	—	Yes

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

Task				Related Document	
	GSS and Standby GSSM CLI	Primary GSSM CLI	Primary GSSM GUI	<i>Cisco Global Site Selector Getting Started Guide Chapter</i>	<i>Cisco Global Site Selector Administration Guide</i>
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
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
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. The 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	
				<i>Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide</i>	<i>Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide</i>
Export and import GSLB configurations in text format	—	Yes	—	Yes	—
Configure locations, regions, and owners	—	Yes	Yes	Yes	Yes
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

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	
				<i>Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide</i>	<i>Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide</i>
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
Perform proximity database management	Yes	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



Configuring the GSS Using the CLI Setup Script

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

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, complete 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. Refer to 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
```

9. The setup script guides you through a series of questions about configuring the device as a GSSM (primary or standby) or as a GSS. 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:
 - 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 these 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 these 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 completed, the software prompts you to perform one of the following actions:
 - **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 configure your GSS devices and resources from the primary GSSM for global server load-balancing, proceed to [Chapter 6, Global Server Load Balancing Summary](#).

Where to Go Next



Accessing the GSS CLI

You can access the GSS CLI by:

- 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 major 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, refer to 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:

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 as was 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:

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 on 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.

Cisco Systems recommends 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. Refer to 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 includes the following procedures:

- [Enabling Remote Access on a GSS Device](#)
- [Accessing the CLI Using a Remote Connection](#)
- [Accessing the CLI Over SSH Using a Private and Public Key Pair](#)

Enabling Remote Access on a GSS Device

To enable SSH, Telnet, or FTP on your GSS device:

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 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
```

- 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:

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

- ip_or_host*—Specifies the IP address or host name 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 host name (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:

```
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
```

- 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
```

To launch the FTP session, specify the IP address or host name 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 host name (for example, myhost.mydomain.com).

For example:

```
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
```

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

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

To enable FTP client access for all users, enter the *all* option. To enable FTP client access for administrative users only, enter the *admin* option. For example:

```
gss.example.com(config)#ftp-client enable all
gss.example.com(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).

Cisco Systems recommends 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:

1. Enter the host name 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:

1. Generate the SSH private key and the corresponding SSH public key as a key pair on a server separate from the GSS. Refer to 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@lmyhost:~/mykey.pub .
myusername@lmyhost 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. To globally enable remote access to the copied private and public keys on the GSS, enter 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 (refer to [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](#).

■ Where to Go Next



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 major sections:

- [Initial Setup Quick Start](#)
- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Setting the System Clock](#)
- [Configuring a Host Name 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 how to:

- Configure the system clock for the GSS device
- Specify a qualified hostname for the GSS device
- Configure Ethernet 0 and Ethernet 1
- Configure a default gateway
- Enter the IP addresses of the name servers (maximum of eight)
- Configure 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. Refer to [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.example.com(config)# interface ethernet 0
gssm1.example.com(config-eth0)# speed 100
gssm1.example.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.example.com(config-eth0)# gss-communications
gssm1.example.com(config-eth0)# exit
gssm1.cisco.com(config)#
```

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

```
gssm1.example.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.	<pre>gssm1.example.com(config-eth1)# exit gssm1.example.com(config)#</pre>
13. Define a default gateway for the GSS device.	<pre>gssm1.example.com(config)# ip default-gateway 172.16.7.18</pre>
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.	<pre>gssm1.example.com(config)# ip name-server 192.168.12.1, 192.168.12.5, 192.168.12.7</pre>
15. Exit global configuration mode.	<pre>gssm1.example.com(config)#exit</pre>
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.	<pre>gssm1.example.com# gss enable gssm-primary</pre>
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.	<pre>gssm2.example.com# gss enable gssm-standby gssm1.example.com</pre>
18. Enable each GSS device as a GSS and direct it to the primary GSSM in your GSS network.	<pre>gss1.example.com# gss enable gss gssm1.example.com</pre>
19. Save your configuration changes to memory.	<pre>gssm1.example.com# copy running-config startup-config</pre>

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 these 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 host name 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, refer to [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 includes the following topics:

- [Setting the Time and Date](#)
- [Setting the Time Zone](#)
- [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:

```
clock set hh:mm:ss MONTH DD YYYY
```

The options and variables are:

- **set**—Sets the device clock to the date and time provided.
- *hh:mm:ss*—The 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*—The 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 timezones, 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:

```
clock timezone timezonename
```

The options and variables are:

- **timezone**—Resets the GSS to synchronize log timestamps to a new timezone.
- *timezonename*— The name of the timezone. Enter **?** to list all supported timezone names.

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

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

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

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

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 [“Synchronizing the GSS System Clock with an NTP Server”](#), while [“Setting the Time and Date”](#) 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.

The syntax for these commands is:

clock update-calendar

clock read-calendar

The options are:

- **update-calendar**— Updates the hardware calendar from the system clock. You can use this command when the system clock is set via NTP and you wish to synchronize the system time with the hardware clock.
- **read-calendar**— Reads the hardware calendar into the system clock. You can use this command when the system clock is set via NTP and you wish to revert back to using the hardware clock.

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:

```
ntp-server ip_or_host
```

The *ip_or_host* variable specifies the IP address or host name of the NTP public time server that provides the clock synchronization. You can specify a maximum of four IP addresses or host names. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (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 4-2](#) describes the fields in the **show clock** command output.

Table 4-2 Field Descriptions for the show clock Command

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

Configuring a Host Name for the GSS Device

By default, the hostname for GSS devices is localhost.localdomain. The host name is used for the command prompts and default configuration filenames. To configure a qualified host name 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 host name 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 messages appears:

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

For the purposes of GSS inter-device 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 host name for the GSS device as a case sensitive text string that contains from 1 to 22 alphanumeric characters.

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

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

To remove the host name 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 autonegotiate, 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:

```
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 Inter-Device 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:

```
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** option 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. Auto-negotiation 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** option 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:

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

The options are:

- **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 include:

- **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 Inter-Device 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 inter-device 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 interfaces 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:

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

or

```
gssml.cisco.com(config)# interface eth1  
gssml.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*—The IP address of the Ethernet interface. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *ip-subnet*—The 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:

```
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 options and variables are:

- **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 host name 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:

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 options and variables are:

- **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 4-3](#) describes the fields in the **show ip routes** output.

Table 4-3 Field Descriptions for show ip routes Command

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

Table 4-3 Field Descriptions for *show ip routes* Command (continued)

Field	Description
Genmask	The subnet mask for the destination network.
Flags	Possible flags include: <ul style="list-style-type: none"> • 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	The 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:

```
dnslookup {hostname | domainname}
```

The variables are:

- *hostname*—The name of the host on the network.
- *domainname*—The name of the domain.

In the example, the **dnslookup** command resolves the host name **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:

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 to do so.

```
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, refer to the *Cisco Global Site Selector Administration Guide*, Chapter 1, Managing GSS Devices from the GUI.

To configure a GSS device as a standby GSSM:

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:

```
gss enable gssm-standby 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 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:

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:

```
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.



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 secure HTTP (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. Refer to the *Cisco Global Site Selector Administration Guide* for information on creating user accounts.

To log in to the primary GSSM GUI:

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://` (secure HTTP) instead of the more common `http://`.

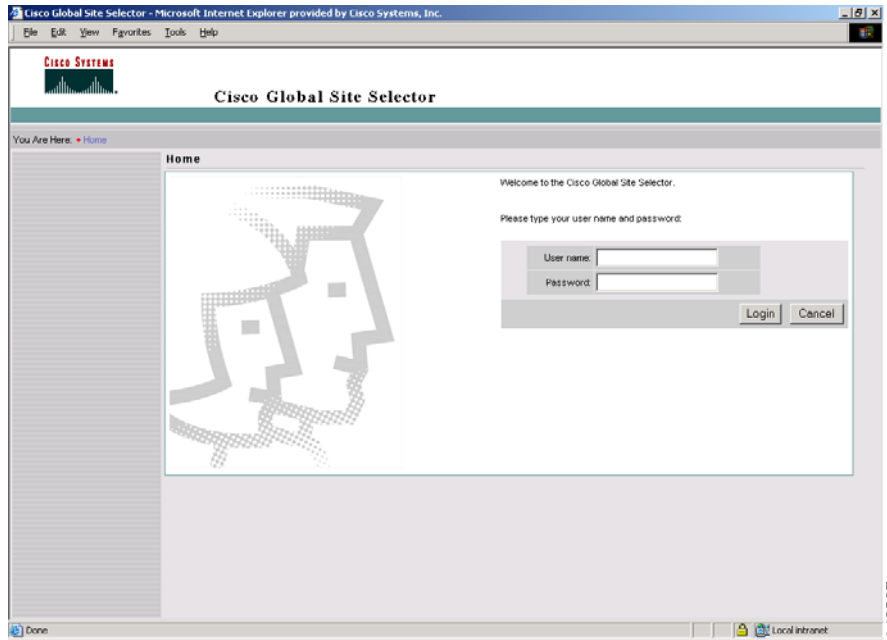
3. Click **Yes** at the prompt to accept (trust) and install the signed certificate from Cisco Systems.

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, refer to the online help included with your browser.

4. To install the signed certificate, if you are using:
 - **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** (Figure 5-2). If this is your first time logging on to the GSSM, use the default account name (admin) and password (default) to access the GUI.

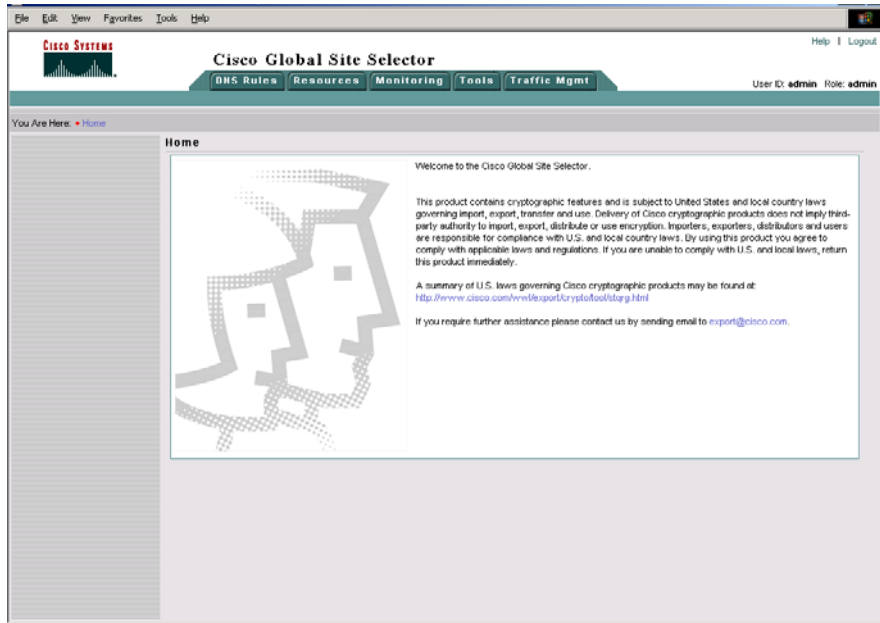
The Primary GSSM Welcome page (Figure 5-2) appears. Refer to the *Cisco Global Site Selector GUI-based Global Server Load-Balancing Configuration Guide* for information on navigating through the primary GSSM GUI.

Figure 5-1 Primary GSSM GUI Login Window



148537

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 redisplay the Primary GSSM GUI Login window (see Figure 5-1).

Activating GSS Devices from the Primary GSSM

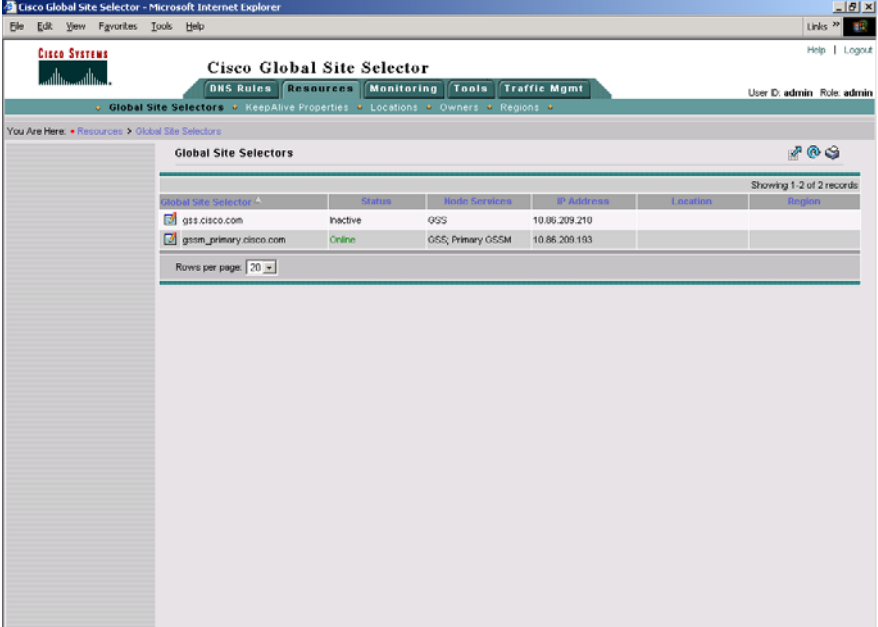
After you configure your GSS devices to function as a standby GSSM or as a GSS, activate those devices from the primary GSSM GUI to add those devices to your GSS network. The standby GSSM and GSS devices are synchronized with the primary GSSM.

To activate a GSS or a standby GSSM from the primary GSSM GUI:

1. Click the **Resources** tab.

2. Click the **Global Site Selectors** navigation link. The Global Site Selectors list page appears (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



The screenshot shows the Cisco Global Site Selector web interface. The browser title is "Cisco Global Site Selector - Microsoft Internet Explorer". The page header includes the Cisco logo and navigation tabs: DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. The user is logged in as "admin". The main content area is titled "Global Site Selectors" and shows a table with the following data:

Global Site Selector	Status	Node Services	IP Address	Location	Region
gss1.cisco.com	Inactive	GSS	10.86.209.210		
gssm_primary.cisco.com	Online	GSS, Primary GSSM	10.86.200.193		

Below the table, it indicates "Showing 1-2 of 2 records" and "Rows per page: 20".

148526

3. Click the **Modify GSS** icon for the first GSS device to activate. The Modifying GSS details page appears (Figure 5-4).

Figure 5-4 Modifying GSS Details Page

The screenshot displays the Cisco Global Site Selector web interface. The browser title is 'Cisco Global Site Selector - Microsoft Internet Explorer'. The page header includes the Cisco Systems logo and navigation tabs for DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. The user is logged in as 'admin'. The main content area is titled 'Modifying GSS: gss.cisco.com' and contains the following configuration details:

General Configuration		Locality	
Name:	gss.cisco.com	Location:	Unspecified
Activate:	<input checked="" type="checkbox"/>	Region:	NA
Node Information		Network Information	
Status:	Inactive	IP Address:	10.00.209.210
Version:	1.0.901.0.13	Hostname:	gss-extreme.cisco.com
Node Services:	GSS	MAC:	00:02:55:b7:73:f1

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

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 (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.

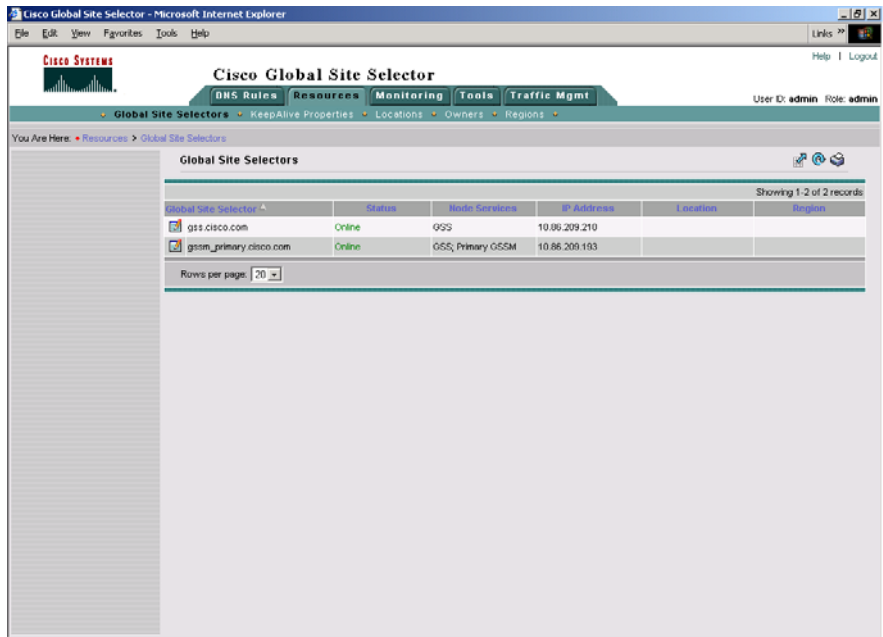


Note

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.

148534

Figure 5-5 Global Site Selectors List Page—Active Status



- 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 6, Global Server Load Balancing Summary](#).

■ Where to Go Next



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 include:

- 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, refer to [Table 1-2 in Chapter 1, Using the CLI and GUI to Manage a GSS Network](#).

Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to 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. Refer to Chapter 9, *Configuring Network Proximity*, for details.



INDEX

A

accessing

CLI [3-1, 3-7](#)

primary GSSM GUI [5-2](#)

remote connection [3-1](#)

serial connection [3-1](#)

activating GSS devices [5-4](#)

audience [xii](#)

autosense, configuring for interface [3-13](#)

C

certificate

accepting [5-2](#)

installing [5-2](#)

trusting [5-2](#)

CLI

accessing [3-1, 3-26](#)

configuring GSS [3-2](#)

default CLI username and password [3-3](#)

direct serial connection [3-1](#)

initial setup quick start [3-2](#)

logging in [3-3, 3-5](#)

private and public key pair [3-7](#)

privileged EXEC mode, enabling [3-3, 3-5](#)

remote connection [3-7](#)

saving session [3-2](#)

clock

displaying [3-10](#)

setting [3-6](#)

synchronizing with NTP server [3-9](#)

D

date

displaying [3-10](#)

setting [3-6](#)

default

password [5-2](#)

username [5-2](#)

documentation

caution and note overview [xvii](#)

conventions [xiv, xvi](#)

organization [xiii](#)

related [xiv](#)

set [xiv](#)

symbols and conventions [xvi](#)

domain name, resolving to IP address [3-25](#)

duplex, configuring for interface [3-14, 3-16](#)

E

Ethernet interface

- autosense, configuring [3-13](#)
- CLI command summary [3-12](#)
- configuring [3-12, 3-13](#)
- duplex, configuring [3-14](#)
- hardware interface status, displaying [3-19](#)
- inter-GSS communication, configuring [3-17](#)
- IP address and subnet mask, configuring [3-18](#)
- keepalive communication, configuring [3-17](#)
- shutting down [3-19](#)
- speed, configuring [3-16](#)
- TCP traffic, dumping [3-20](#)

F

FTP

- disabling [3-5](#)
- enabling [3-5](#)
- IP address or host name, specifying [3-5](#)
- operating status, viewing [3-6](#)

Gglobal server load balancing, summary [6-1](#)

Global Site Selector

- accessing the CLI [3-1, 3-7](#)
- accessing the CLI with private/public key pair [3-7](#)

- activating [5-4](#)
- configured as primary GSSM [3-26](#)
- configured as standby GSSM [3-27](#)
- configuring [3-29](#)
- configuring from CLI [3-2](#)
- date and time, setting [3-6](#)
- direct serial connection [3-1](#)
- enable remote connect [3-3, 3-7](#)
- hardware clock, setting [3-8](#)
- host name, configuring [3-11](#)
- initial configuration with setup script [2-1](#)
- initial setup [2-1](#)
- inter-device communication, configuring [3-17](#)
- network deployment [2-4](#)
- registering [5-4](#)
- remote connection [3-7](#)
- setup configuration decisions [2-4](#)
- setup script, configuring with [2-1](#)
- timezone, setting [3-7](#)

Global Site Selector Manager

- activating [5-4](#)
- date and time, setting [3-6](#)
- default username and password [5-2](#)
- global server load balancing, summary [6-1](#)
- hardware clock, setting [3-8](#)
- host name, configuring [3-11](#)
- initial configuration with setup script [2-1](#)
- initial setup [2-1](#)
- logging on [5-1](#)

- primary GSSM, configuring [3-26](#)
- registering GSS devices [5-4](#)
- setup configuration decisions [2-4](#)
- standby GSSM, configuring [3-27](#)
- timezone, setting [3-7](#)
- URL, secure HTTP [5-2](#)

GSLB configuration tasks

- CLI-based [1-5](#)
- GUI-based [1-5](#)

GSS network

- configuration overview [3-2](#)
- GSS role [3-29](#)
- primary GSSM role [3-26](#)
- setup configuration decisions [2-1, 3-2](#)
- standby GSSM role [3-27](#)
- URL [5-2](#)

GUI

- default username and password [5-2](#)
- logging on [5-1](#)
- logging out [5-4](#)

H

- hardware clock
 - setting [3-8](#)
- hardware interface status, displaying [3-19](#)
- host name
 - configuring for GSS [3-11](#)
 - resolving to IP address [3-25](#)

- HyperTerminal
 - launching [3-1](#)
 - saving session [3-2](#)

I

- initial CSS configuration quick start [3-2](#)
- inter-GSS communication, configuring [3-17](#)
- IP default gateway
 - configuring [3-23](#)
 - deleting [3-23](#)
- IP route
 - configuring [3-23](#)
 - deleting [3-23](#)
 - displaying [3-24](#)
 - routing table, displaying [3-24](#)
 - static route, configuring [3-23](#)

K

- keepalive communication, configuring [3-17](#)

L

- log in
 - certificate [5-2](#)
 - CLI [3-3, 3-5](#)
 - default CLI username and password [3-3](#)
 - default GUI username and password [5-2](#)

logging out [5-4](#)

primary GSSM GUI [5-1](#)

log out [5-4](#)

N

name server, specifying [3-22](#)

network management

tasks using CLI versus GUI [1-1](#)

NTP

enabling [3-9](#)

global sticky mesh requirements [3-9](#)

synchronizing GSS system clock with NTP
server [3-9](#)

P

password

CLI, entering [3-3](#)

default (CLI) [3-3](#)

default (GUI) [5-2](#)

GUI, entering [5-2](#)

private and public key pairs [3-7](#)

privileged EXEC mode, enabling [3-3, 3-5](#)

Q

quick start, initial CSS configuration [3-2](#)

R

registering

GSS with primary GSSM [3-29](#)

standby GSSM with primary GSSM [3-28](#)

registering GSS devices [5-4](#)

remote access

enabling [3-4](#)

FTP [3-5](#)

operating status, viewing [3-6](#)

SSH [3-4](#)

Telnet [3-5](#)

remote connection

accessing CLI [3-7](#)

SSH [3-7](#)

Telnet [3-7](#)

S

secure HTTP address [5-2](#)

setup script

applying [2-5](#)

bypassing [2-1, 2-2](#)

configuring GSS [2-1](#)

configuring GSSM [2-1](#)

shutting down, Ethernet interface [3-19](#)

SSH

disabling [3-4](#)

enabling [3-4](#)

operating status, viewing [3-6](#)
using private and public key pairs [3-7](#)
v1 protocol, enabling [3-4](#)
v2 and v1 protocols [3-4](#)
static IP routing [3-23](#)
GUI, entering [3-3, 5-2](#)

T

TCP traffic, dumping [3-20](#)
Telnet
 disabling [3-5](#)
 enabling [3-5](#)
 IP address, specifying [3-5](#)
 operating status, viewing [3-6](#)
 session port number, changing [3-5](#)
time
 displaying [3-10](#)
 setting [3-6](#)
 timezone, setting [3-7, 3-8](#)
timezone
 displaying [3-10](#)
 setting [3-7](#)

U

username
 CLI, entering [3-3](#)
 default (CLI) [3-3](#)
 default (GUI) [5-2](#)