



Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide

Software Version 2.0
March 2007

Americas 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: 408 527-0883

Text Part Number: OL-10413-01

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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide

© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

Audience xviii

How to Use This Guide xviii

Related Documentation xx

Symbols and Conventions xxi

Obtaining Documentation, Obtaining Support, and Security Guidelines xxiii

CHAPTER 1

Introducing the Global Site Selector 1-1

GSS Overview 1-2

DNS Routing 1-3

DNS Name Servers 1-3

SOA Records 1-4

Negative Caching 1-5

SOA Records and Negative Responses 1-6

DNS Structure 1-7

Request Resolution 1-8

Using the GSS as a DNS Appliance 1-9

Globally Load Balancing with the GSS 1-10

GSS Architecture 1-13

Global Site Selectors and Global Site Selector Managers 1-13

Primary GSSM 1-14

GSS 1-14

Standby GSSM 1-14

- DNS Rules 1-15
- Locations and Regions 1-16
- Owners 1-17
- Source Addresses and Source Address Lists 1-17
- Hosted Domains and Domain Lists 1-18
- Answers and Answer Groups 1-19
 - VIP Answers 1-20
 - Name Server Answers 1-20
 - CRA Answers 1-21
- Keepalives 1-22
 - Multiport Keepalives 1-23
 - ICMP 1-25
 - TCP 1-25
 - HTTP HEAD 1-25
 - KAL-AP 1-26
 - Scripted Keepalive 1-26
 - CRA 1-27
 - Name Server 1-27
 - None 1-27
 - Adjusting Failure Detection Time for Keepalives 1-27
- Balance Methods 1-31
 - Ordered List Method 1-31
 - Round-Robin Method 1-32
 - Weighted Round-Robin Method 1-32
 - Least-Loaded Method 1-32
 - Hashed Method 1-33
 - DNS Race (Boomerang) Method 1-33
 - Balance Method Options for Answer Groups 1-34
- Traffic Management Load Balancing 1-36
 - DNS Sticky GSLB 1-37

Network Proximity GSLB	1-38
DDoS Detection and Mitigation	1-38
Mitigation Rules	1-39
Rate Limits	1-40
Anti-Spoofing Mechanism	1-41
GSS Network Deployment	1-42
Locating GSS Devices	1-43
Locating GSS Devices Behind Firewalls	1-43
Communication Between GSS Nodes	1-44
Deployment Within Data Centers	1-45
GSS Network Management	1-45
CLI-Based GSS Management	1-46
GUI-Based Primary GSSM Management	1-47
Global Server Load-Balancing Summary	1-47
Where to Go Next	1-49

CHAPTER 2

Configuring Resources	2-1
Organizing Your GSS Network	2-2
Logging in to the CLI and Enabling Privileged EXEC Mode	2-3
Configuring Locations and Regions	2-4
Configuring Regions	2-4
Configuring Locations	2-5
Configuring Owners	2-7
Grouping GSS Resources by Location, Region, and Owner	2-8
Displaying Resource Information	2-9
Where to Go Next	2-9

CHAPTER 3

Configuring Source Address Lists 3-1

- Logging in to the CLI and Enabling Privileged EXEC Mode 3-2
- Configuring Source Address Lists 3-2
- Displaying Source Address List Information 3-5
- Where to Go Next 3-5

CHAPTER 4

Configuring Domain Lists 4-1

- Logging in to the CLI and Enabling Privileged EXEC Mode 4-2
- Configuring Domain Lists 4-3
- Displaying Domain List Information 4-5
- Where to Go Next 4-5

CHAPTER 5

Configuring Keepalives 5-1

- Logging in to the CLI and Enabling Privileged EXEC Mode 5-2
- Modifying Global Keepalive Properties 5-3
 - Default Global Keepalive Properties and Settings 5-4
 - Modifying ICMP Global Keepalive Settings 5-6
 - Modifying TCP Global Keepalive Settings 5-8
 - Modifying HTTP HEAD Global Keepalive Settings 5-11
 - Modifying KAL-AP Global Keepalive Settings 5-14
 - Modifying ICMP Global Keepalive Settings 5-16
 - Modifying Scripted Keepalive Global Keepalive Settings 5-18
 - Modifying CRA Global Keepalive Settings 5-20
 - Modifying Name Server Global Keepalive Settings 5-21
- Displaying Global Keepalive Properties 5-21
- Configuring Shared VIP Keepalives 5-22
 - Configuring ICMP Shared Keepalives 5-23
 - Configuring TCP Shared Keepalives 5-23

Configuring HTTP HEAD Shared Keepalives	5-24
Configuring KAL-AP Shared Keepalives	5-25
Configuring Scripted Keepalive Shared Keepalives	5-26
Deleting a Shared Keepalive	5-30
Displaying Shared Keepalive Properties	5-31
Where to Go Next	5-32

CHAPTER 6**Configuring Answers and Answer Groups 6-1**

Configuring and Modifying Answers	6-1
Logging in to the CLI and Enabling Privileged EXEC Mode	6-3
Configuring a VIP-Type Answer	6-3
Configuring Keepalive VIP Answers	6-5
Configuring ICMP Keepalive VIP Answers	6-5
Configuring TCP Keepalive VIP Answer Settings	6-6
Configuring HTTP HEAD Keepalive VIP Answer Settings	6-8
Configuring KAL-AP Keepalive VIP Answer Settings	6-9
Configuring Scripted Keepalive VIP Answers	6-11
Configuring Multiple Keepalives for a VIP Answer Type	6-11
Configuring a CRA-Type Answer	6-13
Configuring a Name Server-Type Answer	6-15
Modifying an Answer	6-16
Displaying Answer Properties	6-18
Suspending an Answer	6-19
Reactivating an Answer	6-19
Suspending or Reactivating All Answers in a Location	6-20
Deleting an Answer	6-21
Configuring and Modifying Answer Groups	6-22
Creating an Answer Group	6-23
Adding Answers to a CRA-Type Answer Group	6-24

- Adding Answers to an NS-Type Answer Group 6-25
- Adding Answers to a VIP-Type Answer Group 6-26
- Modifying an Answer Group 6-27
- Adding or Deleting an Authority Domain in an Answer Group 6-28
- Suspending or Reactivating All Answers in an Answer Group 6-29
- Suspending or Reactivating an Answer in an Answer Group 6-30
- Suspending or Reactivating All Answers in Answer Groups Associated with an Owner 6-31
- Displaying Answer Group Properties 6-32
- Deleting an Answer Group 6-33
- Where to Go Next 6-33

CHAPTER 7

Building and Modifying DNS Rules 7-1

- Logging in to the CLI and Enabling Privileged EXEC Mode 7-2
- Building DNS Rules 7-3
 - Configuring Balance Clauses for a DNS Rule 7-4
 - Configuring Balance Clauses that Use VIP-Type Answer Groups 7-6
 - Configuring Balance Clauses that Use NS-Type Answer Groups 7-8
 - Configuring Balance Clauses that Use CRA-Type Answer Groups 7-10
- Modifying DNS Rules and Balance Clauses 7-12
 - Modifying DNS Rule Properties 7-12
 - Modifying Balance Clause Properties 7-13
- Displaying DNS Rule Properties 7-14
- Suspending a DNS Rule 7-14
- Reactivating a DNS Rule 7-14
- Suspending or Reactivating All DNS Rules Belonging to an Owner 7-15
- Deleting a DNS Rule 7-16
- Configuring DNS Rule Filters 7-17
- Removing DNS Rule Filters 7-17

Delegating to GSS Devices 7-17

Where To Go Next 7-19

CHAPTER 8**Configuring DNS Sticky 8-1**

DNS Sticky Overview 8-2

Local DNS Sticky 8-2

Sticky Database 8-3

Global DNS Sticky 8-5

 GSS Sticky Peer Mesh 8-5

 Sticky Mesh Conflict Resolution 8-7

 Communicating in the Sticky Peer Mesh 8-7

 Logging in to the CLI and Enabling Privileged EXEC Mode 8-9

DNS Sticky Quick Start Guide 8-10

Synchronizing the GSS System Clock with an NTP Server 8-14

Configuring Sticky Using the Primary GSSM CLI 8-16

 Configuring DNS Sticky 8-16

 Enabling Sticky in a DNS Rule 8-20

 Sticky DNS Rule Overview 8-20

 Adding Sticky to a DNS Rule that uses VIP-Type Answer Groups 8-21

 Creating Sticky Groups 8-25

 DNS Sticky Group Overview 8-25

 Creating a DNS Sticky Group 8-27

 Deleting a Sticky Group IP Address Block 8-28

 Deleting a Sticky Group 8-28

 Deleting Entries from the Sticky Database 8-28

 Dumping Sticky Database Entries 8-30

 Running a Periodic Sticky Database Backup 8-32

 Loading Sticky Database Entries 8-33

Disabling DNS Sticky Locally on a GSS for Troubleshooting 8-34

CHAPTER 9

Configuring Network Proximity 9-1

Network Proximity Overview 9-2

Proximity Zones 9-2

Probe Management and Probing 9-3

Proximity Database 9-5

Example of Network Proximity 9-7

Proximity Network Design Guidelines 9-9

Network Proximity Quick Start Guide 9-10

Configuring a Cisco Router as a DRP Agent 9-15

Choosing a Cisco Router as a DRP Agent 9-16

Configuring the DRP Agent 9-16

Cisco IOS Release 12.1 Interoperability Considerations 9-17

Logging in to the CLI and Enabling Privileged EXEC Mode 9-18

Synchronizing the GSS System Clock with an NTP Server 9-18

Creating Zones Using the Primary GSSM CLI 9-20

Configuring a Proximity Zone 9-20

Deleting a Proximity Zone 9-21

Associating a Proximity Zone With a Location 9-21

Associating a Proximity-Based Location with an Answer 9-23

Configuring Proximity Using the Primary GSSM CLI 9-24

Configuring Proximity 9-24

Creating DRP Keys 9-29

Deleting DRP Keys 9-30

Adding a Proximity Balance Clause to a DNS Rule 9-30

Proximity Balance Clause Overview 9-30

Adding Proximity to a DNS Rule that uses VIP-Type Answer Groups 9-31

Creating Proximity Groups 9-34

Proximity Group Overview 9-35

Creating a Proximity Group 9-36

Playing Static Proximity Group Configurations	9-37
Deleting a Proximity Group IP Address Block	9-38
Deleting a Proximity Group	9-39
Configuring Static Proximity Database Entries	9-39
Adding Static Proximity Entries	9-39
Deleting Static Entries from the Proximity Database	9-41
Deleting Entries from the Proximity Database	9-42
Dumping Proximity Database Entries to a File	9-43
Running a Periodic Proximity Database Backup	9-45
Loading Proximity Database Entries	9-46
Initiating Probing for a D-proxy Address	9-47
Disabling Proximity Locally on a GSS for Troubleshooting	9-47
Where to Go Next	9-48

CHAPTER 10**Configuring DDoS Prevention 10-1**

Logging in to the CLI and Enabling Privileged EXEC Mode	10-2
Enabling or Disabling DDoS Detection and Mitigation	10-2
Modifying or Restoring Rate Limits	10-3
Setting a Scaling Factor	10-5
Configuring Trusted or Spoofed D-proxies	10-5
Enabling or Disabling Mitigation Rule Checks	10-6
Configuring a Global Domain Name	10-7
Configuring Maximum Entries in the DDoS Database	10-7
Executing a Saved DDoS Configuration File	10-8
Configuring Peacetime Learning	10-8
Starting Peacetime Learning	10-9
Stopping Peacetime Learning	10-9
Saving Peacetime Learning	10-10

- Showing Peacetime Learning 10-10
- Erasing Peacetime Learning 10-11
- Setting the Location for the Peacetime File 10-11
- Applying Peacetime Values 10-12
- Managing Your DDoS Configuration 10-12
 - Copying a DDoS Configuration to Disk 10-12
 - Clearing a DDoS Configuration 10-13
- Restoring DDoS Defaults 10-13
- Where to Go Next 10-14

CHAPTER 11

Creating and Playing GSLB Configuration Files 11-1

- GSLB Configuration File Overview 11-2
- Creating a GSLB Configuration File 11-3
- Securely Copying GSLB Configuration Files 11-4
- Modifying a GSLB Configuration File 11-5
 - File Modification Guidelines 11-5
 - File Modification Workflow 11-6
- Playing a GSLB Configuration File 11-7
- Where to Go Next 11-8

CHAPTER 12

Displaying Global Server Load-Balancing Configuration Information 12-1

- Displaying Resource Configuration Information 12-2
 - Displaying Location Configuration Information 12-2
 - Displaying Owner Configuration Information 12-2
 - Displaying Region Configuration Information 12-3
 - Displaying Zone Configuration Information 12-3
- Displaying Source Address Configuration Information 12-4
- Displaying Domain Configuration Information 12-5

Displaying Keepalive Configuration Information	12-6
Displaying Shared Keepalive Configuration Information	12-9
Displaying Answer Configuration Information	12-11
Displaying Answer Group Configuration Information	12-13
Displaying DNS Rule Configuration Information	12-14
Displaying DNS Sticky Configuration Information	12-16
Displaying Global Sticky Group Information	12-16
Displaying Global Sticky Properties Information	12-17
Displaying DNS Proximity Configuration Information	12-17
Displaying Global Proximity Group Information	12-18
Displaying Global Proximity Properties Information	12-18
Where to Go Next	12-20

CHAPTER 13**Displaying GSS Global Server Load-Balancing Statistics 13-1**

Displaying Global Server Load-Balancing Statistics from the CLI	13-2
Displaying the Status of the Boomerang Server on a GSS	13-3
Displaying the Status of the DNS Server on a GSS	13-4
Displaying Answer Statistics	13-5
Displaying Answer Group Statistics	13-6
Displaying Domain Statistics	13-8
Displaying Domain List Statistics	13-9
Displaying Global Statistics	13-10
Displaying DNS Rule Proximity Statistics	13-12
Displaying DNS Rule Statistics	13-12
Displaying Source Address Statistics	13-14
Displaying Source Address List Statistics	13-15
Displaying DNS Rule Sticky Statistics	13-16
Displaying the Status of the DRP Agent on a GSS	13-17
Displaying DDoS Statistics on a GSS	13-18

- Displaying DDoS Attack Statistics 13-18
- Displaying DDoS Anti-Spoofing Statistics 13-19
- Displaying DDoS Failed DNS Queries 13-20
- Displaying DDoS Rate-Limit Values 13-22
- Displaying DDoS Running Configuration 13-23
- Displaying DDoS Statistics 13-24
- Displaying DDoS Status 13-27
- Displaying the Status of Keepalives on a GSS 13-28
 - Displaying CRA Keepalive Statistics 13-28
 - Displaying Global Keepalive Statistics 13-30
 - Displaying HTTP HEAD Keepalive Statistics 13-34
 - Displaying ICMP Keepalive Statistics 13-35
 - Displaying KAL-AP Keepalive Statistics 13-37
 - Displaying Scripted Keepalive Statistics 13-38
 - Displaying Name Server Keepalive Statistics 13-41
 - Displaying TCP Keepalive Statistics 13-42
 - Displaying Keepalive Answer Type Statistics 13-43
- Displaying Network Proximity Statistics on a GSS 13-45
 - Displaying DNS Rule Proximity Statistics 13-45
 - Displaying Proximity Database Statistics 13-46
 - Displaying Proximity Group Statistics 13-48
 - Displaying Proximity Lookup Statistics 13-49
 - Displaying Proximity Probe Transfer Statistics 13-50
 - Displaying Proximity Status 13-53
 - Displaying Proximity Group Configuration 13-53
 - Displaying Proximity Database Status 13-54
- Displaying DNS Sticky Statistics on a GSS 13-55
 - Displaying DNS Rule Sticky Statistics 13-56
 - Displaying Sticky Statistics 13-56
 - Displaying Global Sticky Statistics 13-58

Displaying Global Sticky Mesh Statistics	13-63
Displaying Sticky Group Statistics	13-65
Displaying the Sticky Status	13-67
Displaying the Sticky Database Status	13-69
Displaying the Global Sticky Operating Status	13-70
Displaying Global Sticky Mesh Operating Status	13-77
Displaying Sticky Group Configuration	13-86
Clearing GSS Global Server Load-Balancing Statistics	13-87
Displaying Global Server Load-Balancing Statistics from the GUI	13-89
Displaying Answer Status and Statistics	13-89
Displaying Answer Hit Counts	13-90
Displaying Answer Keepalive Statistics	13-91
Displaying the Answer Status	13-94
Displaying DNS Rule Statistics	13-95
Displaying Domain Hit Counts	13-97
Displaying Global Statistics	13-98
Displaying Source Address Statistics	13-100
Displaying DDoS Statistics	13-101
Monitoring Traffic Management Statistics	13-106
Displaying Proximity Rule Hit Count Statistics	13-106
Displaying Proximity Database Statistics	13-108
Displaying Proximity Lookup Statistics	13-110
Displaying Proximity Probe Management Statistics	13-111
Displaying Sticky Rule Hit Statistics	13-114
Displaying Sticky Database Statistics	13-115
Displaying Global Sticky Mesh Statistics	13-117

APPENDIX A**Primary GSSM Global Server Load-Balancing Error Messages** A-1

Answer Error Messages A-2

Answer Group Error Messages A-4

- Domain List Error Messages **A-6**
- DNS Rule Error Messages **A-9**
- KeepAlive Error Messages **A-15**
- Location Error Messages **A-18**
- Network Error Messages **A-18**
- Owner Error Messages **A-19**
- Proximity Error Messages **A-19**
- Region Error Messages **A-24**
- Source Address List Error Messages **A-24**
- Sticky Error Messages **A-26**
- User Account Error Messages **A-27**
- User Views Error Messages **A-28**

APPENDIX B

Sticky and Proximity XML Schema Files **B-1**

- Sticky XML Schema File Contents **B-2**
- Proximity XML Schema File Contents **B-4**

GLOSSARY

INDEX



Preface

This guide includes information on using the command-line interface (CLI) to configure the Cisco Global Site Selector (GSS) to perform global server load balancing. Certain global server load-balancing tasks require that you use the CLI; other tasks require that you use the GUI. In most cases, you have the option of using either the CLI or the GUI at the primary Global Site Selector Manager (GSSM). In cases where you must use the GUI to perform a particular task (configuring DNS rule filters, for example), the task is listed and a reference to the appropriate chapter in the *Global Site Selector GUI-Based Global Load-Balancing Configuration Guide* is provided.

This preface contains the following major sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

Audience

To use this configuration guide, you should be familiar with the GSS platform hardware. 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, Introducing the Global Site Selector	Describes the basic concepts of the GSS product and important GSS-related terms.
Chapter 2, Configuring Resources	Describes how to organize resources on your GSS network as locations, regions, and owners.
Chapter 3, Configuring Source Address Lists	Describes how to create and modify source address lists.
Chapter 4, Configuring Domain Lists	Describes how to create and modify domain lists.
Chapter 5, Configuring Keepalives	Describes how to modify global keepalive parameters and create shared keepalives.
Chapter 6, Configuring Answers and Answer Groups	Describes how to create GSS answers and answer groups.
Chapter 7, Building and Modifying DNS Rules	Describes how to construct the DNS rules that govern all global server load balancing on your GSS network.
Chapter 8, Configuring DNS Sticky	Describes how to configure local and global DNS sticky for GSS devices in your network.
Chapter 9, Configuring Network Proximity	Describes how to configure proximity for GSS devices in your network.

Chapter/Title	Description
Chapter 10, Configuring DDoS Prevention	Describes how to configure the GSS to prevent Distributed Denial of Service (DDoS) attacks.
Chapter 11, Creating and Playing GSLB Configuration Files	Describes how to create, modify, and play GSLB configuration files.
Chapter 12, Displaying Global Server Load-Balancing Configuration Information	Describes the commands that you use to display information about the global server load-balancing configuration on your GSS network.
Chapter 13, Displaying GSS Global Server Load-Balancing Statistics	Describes the tools that you use to display the status of global load balancing on your GSS network.
Appendix A, Primary GSSM Global Server Load-Balancing Error Messages	Describes the primary GSSM global server load-balancing operating error messages.
Appendix B, “Sticky and Proximity XML Schema Files”	Describes how you use the two XML schema files, included with the GSS, to describe and validate the sticky XML and proximity XML output files.

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>	Provides 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 system hardware.
<i>Regulatory Compliance and Safety Information for the Cisco Global Site Selector</i>	Provides regulatory compliance and safety information for the GSS platform.
<i>Release Note for the Cisco Global Site Selector</i>	Provides information on operating considerations, caveats, and new CLI commands for the GSS software.
<i>Cisco Global Site Selector Getting Started Guide</i>	Provides information on getting your GSS set up, configured, and ready to perform global server load balancing.
<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 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 Command Reference</i>	Provides an alphabetical list, by mode, of all GSS command-line interface (CLI) commands including syntax, options, and related commands. This document also describes how to use the CLI interface.

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 set of characters. Strings that include spaces (for example, “name 1”) must be in quotes.

Screen examples use the following conventions:

screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .
<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 you to enter a keystroke or act on a GUI element.
Courier text	Indicates text that appears in a command line, including the CLI prompt.
Courier bold text	Indicates commands and text you enter in a command line.
<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.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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



CHAPTER 1

Introducing the Global Site Selector

This chapter describes the Cisco Global Site Selector (GSS) and introduces you to the terms and concepts necessary to help you understand and operate the GSS.

This chapter contains the following major sections:

- [GSS Overview](#)
- [DNS Routing](#)
- [Using the GSS as a DNS Appliance](#)
- [Globally Load Balancing with the GSS](#)
- [GSS Architecture](#)
- [DDoS Detection and Mitigation](#)
- [GSS Network Deployment](#)
- [GSS Network Management](#)
- [Global Server Load-Balancing Summary](#)
- [Where to Go Next](#)

For more information on DNS-based global server load balancing (GSLB) as it applies to the GSS, see the *Business Case for Global Server Load Balancing* white paper available on Cisco.com at this URL:

http://www.cisco.com/en/US/product/hw/contnetw/ps4162/prod_white_papers_list.html

GSS Overview

Server load-balancing devices, such as the Cisco Content Services Switch (CSS) and Cisco Content Switching Module (CSM) that are connected to a corporate LAN or the Internet, can balance content requests among two or more servers containing the same content. Server load-balancing devices ensure that the content consumer is directed to the host that is best suited to handle that consumer's request.

Organizations with a global reach or businesses that provide web and application hosting services require network devices that can perform complex request routing to two or more redundant, geographically dispersed data centers. These network devices need to provide fast response times and disaster recovery and failover protection through global server load balancing, or GSLB.

The Cisco Global Site Selector (GSS) platform allows you to leverage global content deployment across multiple distributed and mirrored data locations, optimizing site selection, improving Domain Name System (DNS) responsiveness, and ensuring data center availability.

The GSS is inserted into the traditional DNS routing hierarchy and is closely integrated with the Cisco CSS, Cisco CSM, or third-party server load balancers (SLBs) to monitor the health and load of the SLBs in your data centers. The GSS uses this information and user-specified routing algorithms to select the best-suited and least-loaded data center in real time.

The GSS can detect site outages, ensuring that web-based applications are always online and that customer requests to data centers that suddenly go offline are quickly rerouted to available resources.

The GSS offloads tasks from traditional DNS servers by taking control of the domain resolution process for parts of your domain name space, responding to requests at a rate of thousands of requests per second.

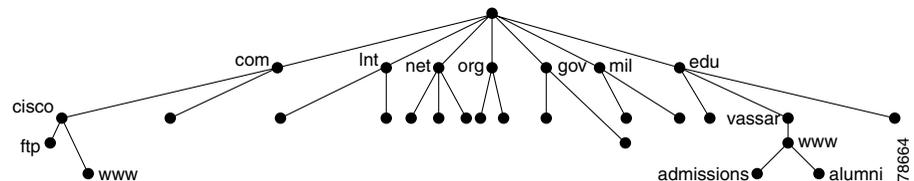
DNS Routing

This section explains some of the key DNS routing concepts behind the GSS.

Since the early 1980s, content routing on the Internet has been handled using the Domain Name System (DNS), a distributed database of host information that maps domain names to IP addresses. Almost all transactions that occur across the Internet rely on DNS, including electronic mail, remote terminal access such as Telnet, file transfers using the File Transfer Protocol (FTP), and web surfing. DNS uses alphanumeric hostnames instead of numeric IP addresses that bear no relationship to the content on the host.

With DNS, you can manage a nearly infinite number of hostnames referred to as the domain name space (see [Figure 1-1](#)). DNS allows local administration of segments (individual domains) of the overall database, but allows for data in any segment to be available across the entire network. This process is referred to as *delegation*.

Figure 1-1 Domain Name Space



This section contains the following topics:

- [DNS Name Servers](#)
- [DNS Structure](#)
- [Request Resolution](#)

DNS Name Servers

Information about the domain name space is stored on name servers that are distributed throughout the Internet. Each server stores the complete information about its small part of the total domain name space. This space is referred to as a DNS *zone*. A zone file contains DNS information for one domain (“mycompany.com”) or subdomain (“gslb.mycompany.com”).

The DNS information is organized into lines of information called resource records. Resource records describe the global properties of a zone and the hosts or services that are part of the zone. They are stored in binary format internally for use by the DNS software. However, resource records are sent across the network in a text format while they perform zone transfers.

Resource records are composed of various types of records including:

- Start of Authority (SOA)
- Name Service (NS)
- Address (A)
- Host Information (HINFO)
- Mail Exchange (MX)
- Canonical Name (CNAME)
- Pointer (PTR)

This document deals primarily with SOA and NS record types. For a detailed description of the other supported record types, as well as instructions for configuring resource records, see the *Cisco CNS Network Registrar User's Guide*. You can also consult RFC 1034 and 1035 for additional background information on resource records.

This section contains the following topics:

- [SOA Records](#)
- [Negative Caching](#)
- [SOA Records and Negative Responses](#)

SOA Records

At the top-level of a domain, the name database must contain a Start of Authority (SOA) record that identifies the best source of information for data within the domain. The SOA record also contains the current version of the DNS database and defines the behavior of a particular DNS server.

Each subdomain that is separately nameserved must have at least one corresponding NS record since name servers use these records to find each other. The zone is the region of the namespace that has a separate SOA. The format for this record is shown in the following example:

```
DOMAIN.NAME. IN SOA Hostname.Domain.Name. Mailbox.Domain.Name.  
1 ; serno (serial number)  
86400 ; refresh in seconds (24 hours)  
7200 ; retry in seconds (2 hours)  
2592000 ; expire in seconds (30 days)  
345600 ; TTL in seconds (4 days)
```

Negative Caching

Busy servers have to handle hundreds or even thousands of name resolution requests each second. Therefore, it is essential that DNS server implementations employ mechanisms to improve their efficiency and cut down on unnecessary name resolution requests since each of these requests takes time and resources to resolve. Such requests also take internetwork bandwidth away from the business of transferring data.

Caching is one of the most important of these efficiency mechanisms. Caching refers to an area of memory set aside for storing information that has been recently obtained so it can be used again. In the case of DNS, caching is used by DNS name servers to store the results of recent name resolution and other requests, so that if the request occurs again it can be satisfied from the cache without requiring another complete run of the name resolution process. For more information, see the [“Request Resolution”](#) section.

Negative caching refers to the functions within a name server that maintain the non-existence of specific DNS records. Negative caching stores negative results and reduces the response time for negative answers. It also reduces the number of messages sent between resolvers and name servers, thus reducing the amount of overall network traffic. Maintaining a negative cache state allows the system to quickly return a failure condition when a lookup attempt is retried.

Within the SOA record, the numeric Time to Live (TTL) fields control the frequency with which name servers poll each other to get information updates. For example, the TTL fields control the frequency with which the name servers poll each other to determine how long the data is cached. DNS allows name servers to distribute, and resolvers to cache, negative results with TTLs.

SOA record TTLs are required when forming negative responses for DNS queries since negative caching stores the knowledge that a resource record set (RRset), or domain name does not exist, or does not provide an answer.



Note An RRset is a group of records that contain the same label, class, and type, but contains different data.

The most common negative responses indicate that a particular RRset does not exist in the DNS. Name errors (NXDOMAIN) are indicated by the presence of *name error* in the response code (RCODE) field, while NODATA is indicated by an answer with the RCODE sent to NOERROR and no relevant answers in the answer section. For such negative responses, GSS appends the SOA record of the zone in the authority section of the response.

SOA Records and Negative Responses

When the SOA record needs to be included in the negative response, the corresponding name server is queried for the SOA for the corresponding domain by the GSS. This SOA response is cached for a period mentioned in the minimum field of the SOA record. For all negative responses during this period, the cached SOA record is used, rather than querying the name server for the same domain.



Note In GSS v2.0, the default behavior is to reply to queries with negative responses, whereas in GSS v1.3.3, the default is not to respond to negative queries.

If the GSS fails to obtain the SOA, the negative response is the appropriate error code. When using the cached SOA, the TTL of the negative response will be decremented by the time (in seconds) since the SOA was cached. This process is similar to the manner in which a caching-only name server decrements the TTL of the cached records.



Note If you want to upgrade to GSS v2.0 but do not need any new DNS features and do not care what type of negative response will be returned for queries, you do not need to perform any additional SOA configuration. In such cases, GSS returns a type 3 negative response which does not contain the SOA information when the request cannot be answered.

To configure SOA records on the GSS to use in the negative response, you need to configure an NS answer that specifies the IP address of the authority name server for the domain and the domains hosted on the name server. See the [“Adding or Deleting an Authority Domain in an Answer Group”](#) section in [Chapter 6](#), for more details.

DNS Structure

End users who require data from a particular domain or machine generate a recursive DNS request on their client that is sent first to the local name service (NS), also referred to as the *D-proxy*. The D-proxy returns the IP address of the requested domain to the end user.

The DNS structure is based on a hierarchical tree structure that is similar to common file systems. The key components in this infrastructure are as follows:

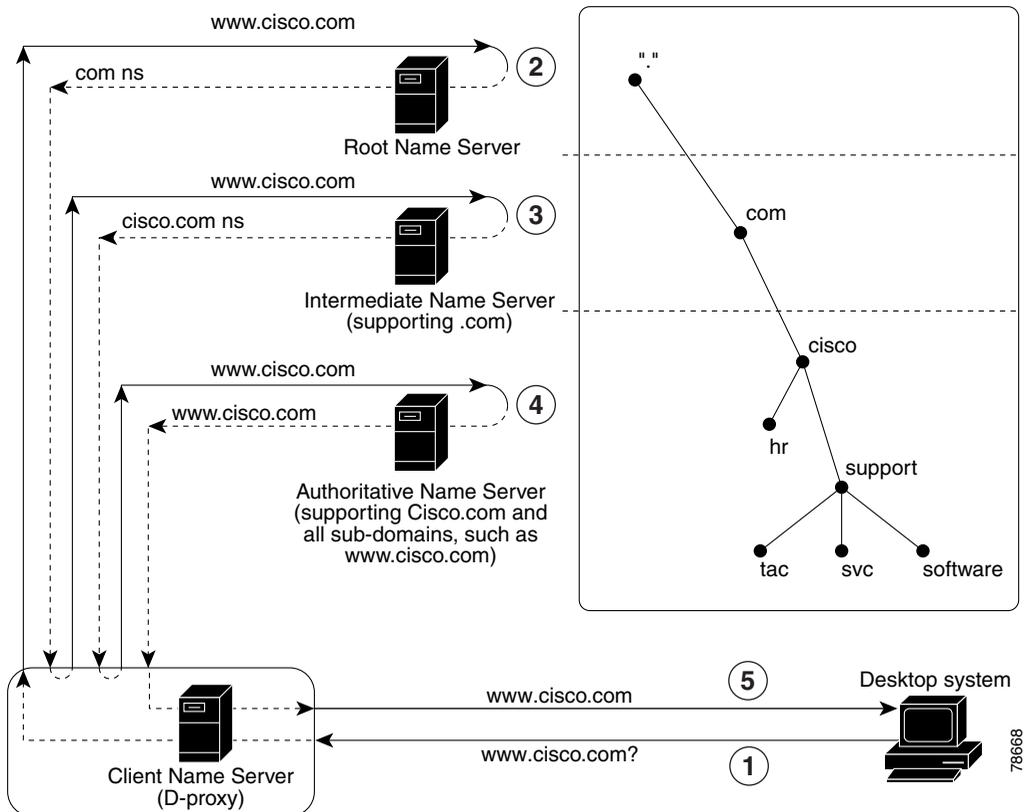
- **DNS Resolvers**—Clients that access client name servers.
- **Client Name Server**—Server that runs DNS software that has the responsibility of finding the requested web site. The client name server is also referred to as the client DNS proxy (D-proxy).
- **Root Name Servers**—Server that resides at the top of the DNS hierarchy. The root name server knows how to locate every extension after the period (.) in the hostname. There are many top-level domains. The most common top-level domains include .org, .edu, .net, .gov, and .mil. Approximately 13 root servers worldwide handle all Internet requests.
- **Intermediate Name Server**—Server that is used for scaling purposes. When the root name server does not have the IP address of the authoritative name server, it sends the requesting client name server to an intermediate name server. The intermediate name server then refers the client name server to the authoritative name server.
- **Authoritative Name Server**—Server that is run by an enterprise or outsourced to a service provider and is authoritative for the domain requested. The authoritative name server responds directly to the client name server (not to the client) with the requested IP address.

Request Resolution

If the local D-proxy does not have the information requested by the end user, it sends out iterative requests to the name servers that it knows are authoritative for the domains close to the requested domain. For example, a request for `www.cisco.com` causes the local D-proxy to check first for another name server that is authoritative for `www.cisco.com`.

Figure 1-2 summarizes the sequence performed by the DNS infrastructure to return an IP address when a client tries to access the `www.cisco.com` website.

Figure 1-2 DNS Request Resolution



78668

1. The resolver (client) sends a query for `www.cisco.com` to the local client name server (D-proxy).
2. The local D-proxy does not have the IP address for `www.cisco.com` so it sends a query to a root name server (“.”) asking for the IP address. The root name server responds to the request by doing one of the following:
 - Referring the D-proxy to the specific name server that supports the `.com` domain.
 - Sending the D-proxy to an intermediate name server that knows the address of the authoritative name server for `www.cisco.com`. This method is referred to as an iterative query.
3. The local D-proxy sends a query to the intermediate name server that responds by referring the D-proxy to the authoritative name server for `cisco.com` and all the associated subdomains.
4. The local D-proxy sends a query to the `cisco.com` authoritative name server that is the top-level domain. In this example, `www.cisco.com` is a sub-domain of `cisco.com`, so this name server is authoritative for the requested domain and sends the IP address to the name server (D-proxy).
5. The name server (D-proxy) sends the IP address (`172.16.56.76`) to the client browser. The browser uses this IP address and initiates a connection to the `www.cisco.com` website.

Using the GSS as a DNS Appliance

GSS load balances geographically distributed data centers based on DNS requests. It also load balances any DNS-capable device that can be registered in the DNS system, such as origin servers, or third-party SLBs. For more information, see the [“Globally Load Balancing with the GSS”](#) section.

Typically, the GSS operates at a sublevel within the DNS hierarchy, responding only to a certain subset of DNS queries. Customers are then required to use a DNS server to process the other types of DNS queries.

With the v2.0 release, GSS product capabilities have been enhanced to allow the GSS to migrate to the top level of the DNS hierarchy. This is accomplished through a product coupling with the Cisco Network Registrar (CNR) which permits the GSS to behave like a DNS appliance, thus simplifying the process of managing and configuring the DNS infrastructure.

The coupling can be viewed as two separate subsystems running on the same physical hardware with the GSS acting as the front-end DNS server and receiving all DNS requests.

Each query is processed as follows, depending upon its type:

- **A Queries**— The GSS processes these queries and responds if it finds a reply for the query. If it fails to find a reply, it queries the CNR subsystem for a reply. The CNR reply is then forwarded to the D-Proxy.
- **All other Queries**— These queries are forwarded to the CNR subsystem. The response from the CNR subsystem is forwarded back to the D-Proxy. If the response contains *A* records in the Additional Section, the GSS may perform its own query processing and modify the Additional Section of the Response to provide a load-balanced *A* records in the Additional Section.

For more information on CNR and GSS and their interaction and instructions on how to obtain and install a CNR license on the GSS, see the *Global Site Selector Administration Guide*.

Globally Load Balancing with the GSS

The GSS addresses critical disaster recovery requirements by globally load balancing distributed data centers. The GSS coordinates the efforts of geographically dispersed SLBs in a global network deployment for the following Cisco products:

- Cisco Content Services Switch 11500, 11000, or 11150
- Cisco Content Switching Module (CSM) for the Catalyst 6500 series switches
- Cisco LocalDirector
- Cisco IOS SLB
- Cisco router using the DRP agent for network proximity
- Any server that is capable of responding to HTTP HEAD, ICMP, or TCP requests
- Cisco router with cache modules
- Cisco Cache Engines

The GSS supports over 4000 separate virtual IP (VIP) addresses. It coordinates the activities of SLBs by acting as the authoritative DNS server for those devices under its control.

Once the GSS becomes responsible for GSLB services, the DNS process migrates to the GSS. The DNS configuration is the same process as described in the “Request Resolution” section. The only exception is that the NS-records point to the GSSs located at each data center. The GSS determines which data center site should receive the client traffic.

As the authoritative name server for a domain or subdomain, the GSS considers the following additional factors when responding to a DNS request:

- Availability—Servers that are online and available to respond to the query
- Proximity—Server that responded to a query most quickly
- Load—Type of traffic load handled by each server in the domain
- Source of the Request—Name server (D-proxy) that requests the content
- Preference—First, second, or third choice of the load-balancing algorithm to use when responding to a query

This type of global server load balancing ensures that the end users are always directed to resources that are online, and that requests are forwarded to the most suitable device, resulting in faster response time for users.

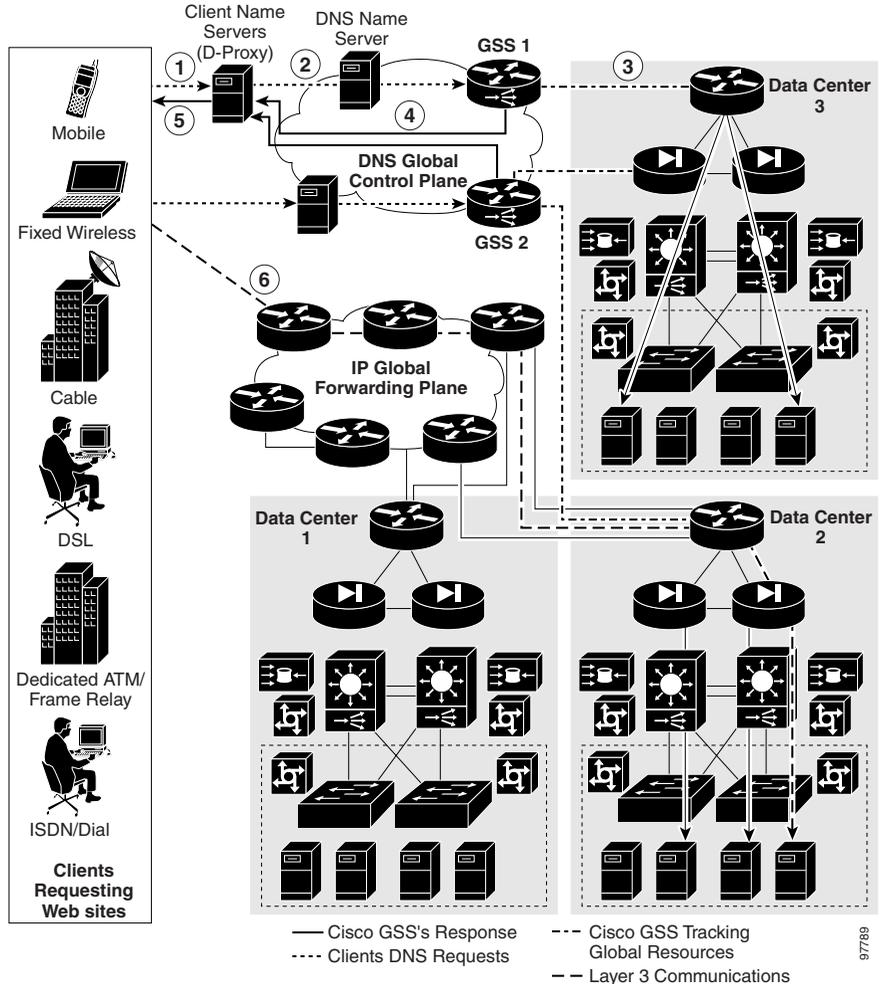
When resolving DNS requests, the GSS performs a series of distinct operations that take into account the resources under its control and return the best possible answer to the requesting client’s D-proxy.

Figure 1-3 outlines how the GSS interacts with various clients as part of the website selection process to return the IP address of the requested content site.

1. A client starts to download an updated version of software from `www.cisco.com` and types **www.cisco.com** in the location or address field of the browser. This application is supported at three different data centers.
2. The DNS global control plane infrastructure processes the request and the request arrives at a GSS device.
3. The GSS sends the IP address of the “best” server load balancer to the client, in this case the SLB at Data Center 2.
4. The web browser processes the transmitted IP address.
5. The client is directed to the SLB at Data Center 2 by the IP control and forwarding plane.

- The GSS offloads the site selection process from the DNS global control plane. The request and site selection are based on the load and health information with user-controlled load-balancing algorithms. The GSS selects in real time a data center that is available and not overloaded.

Figure 1-3 GLSB Using the Cisco Global Site Selector



GSS Architecture

This section describes the key components of a GSS deployment, including hardware and software, as well as GSS networking concepts. It contains the following topics:

- [Global Site Selectors and Global Site Selector Managers](#)
- [DNS Rules](#)
- [Locations and Regions](#)
- [Owners](#)
- [Source Addresses and Source Address Lists](#)
- [Hosted Domains and Domain Lists](#)
- [Answers and Answer Groups](#)
- [Keepalives](#)
- [Balance Methods](#)
- [Traffic Management Load Balancing](#)

Global Site Selectors and Global Site Selector Managers

All GSS devices in the network, including the primary GSSM and standby GSSM, are delegated authority for domains, respond to DNS queries and perform keepalives, and use their local CLI for basic network management. All GSS devices depend on the primary GSSM to provide centralized, shared global server load-balancing functionality.

This section contains the following topics:

- Primary GSSM
- GSS
- Standby GSSM

Primary GSSM

The primary GSSM is a GSS that runs the GSS software. It performs content routing in addition to centralized management and shared global server load-balancing functions for the GSS network.

The primary GSSM hosts the embedded GSS database that contains configuration information for all your GSS resources, such as individual GSSs and DNS rules. All connected GSS devices report their status to the primary GSSM.

On the primary GSSM, you monitor and administer GSS devices using either of the following methods:

- CLI commands
- GUI (graphical user interface) functions, as described in the *Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide*

All configuration changes are communicated automatically to each device managed by the primary GSSM.

Any GSS device can serve as the single, primary GSSM on a configured system.

GSS

The GSS runs the GSS software and routes DNS queries based on DNS rules and conditions configured using the primary GSSM.

Each GSS is known to and synchronized with the primary GSSM.

You manage each GSS individually through its command-line interface (CLI). Support for the graphical-user interface (GUI) is not available on a GSS or on a standby GSSM.

Standby GSSM

The standby GSSM is a GSS that runs the GSS software and routes DNS queries based on DNS rules and conditions configured using the primary GSSM. Additionally, the standby GSSM is configured to function as the primary GSSM if the designated primary GSSM goes offline or becomes unavailable to communicate with other GSS devices.

When the standby GSSM operates as the interim primary GSSM, it contains a duplicate copy of the embedded GSS database currently installed on the primary GSSM. Both CLI and GUI support are also available on the standby GSSM once

you configure it as the interim primary GSSM. While operating as the primary GSSM, you can monitor GSS behavior and make configuration changes, as necessary.

Any configuration or network changes that affect the GSS network are synchronized between the primary and the standby GSSM so the two devices are never out of sequence.

To enable the standby GSSM as the primary GSSM, use the **gssm standby-to-primary** CLI command. Ensure that your original primary GSSM is offline before you attempt to enable the standby GSSM as the new primary GSSM.

**Caution**

Having two primary GSSMs active at the same time may result in the inadvertent loss of configuration changes for your GSS network. If this dual primary GSSM configuration occurs, the two primary GSSMs revert to standby mode and you must reconfigure one of the GSSMs as the primary GSSM.

The standby GSSM can temporarily assume the role of the primary GSSM if the primary GSSM is unavailable (for example, you need to move the primary GSSM or you want to take it offline for repair or maintenance). Switching roles between the designated primary GSSM and the standby GSSM is intended to be a temporary GSS network configuration until the original primary GSSM can be brought back online. Once the original primary GSSM is available, reassign the two GSSMs to their original roles in the GSS network as described in the *Cisco Global Site Selector Administration Guide*.

DNS Rules

At the primary GSSM, you can configure DNS rules to do the following:

- Provide you with centralized command and control of how the GSS globally load balances a given hosted domain
- Define the IP addresses to send to the client's name server (D-proxy)
- Define the recovery method to use (using a maximum of three load-balance clauses)

Each DNS rule determines how the GSS responds to each query it receives by matching requests received from a known source, or D-proxy, to the most suitable member of a collection of name servers or virtual IP addresses (VIPs).

Each DNS rule takes into account the following variables:

- The source IP address of the requesting D-proxy.
- The requested hosted domain.
- An answer group, which is a group of resources considered for the response.
- A balance method, which is an algorithm for selecting the best server; a balance method and an answer group makes up a clause.
- Advanced traffic management load-balancing functions such as DNS sticky and network proximity.

A DNS rule defines how a request is handled by the GSS by answering the following question:

When traffic arrives from a DNS proxy, querying a specific domain name, which resources should be considered for the response, and how should they be balanced?

Each GSS network supports a maximum of 4000 DNS rules.

A maximum of three possible response answer group and balance method clauses are available for each DNS rule. Each clause specifies that a particular answer group serve the request and a specific balance method be used to select the best resource from that answer group. These clauses are evaluated in order, with parameters established to determine when a clause should be skipped if the first answer group and balance method specified does not yield an answer, and the next clause is to be used.

See [Chapter 7, Building and Modifying DNS Rules](#), for procedures on constructing the DNS rules that govern all global server load balancing on your GSS network.

Locations and Regions

As your GSS network expands, the job of organizing and administering your GSS resources—locations, regions, answers and answer groups, domain lists, and DNS rules—becomes more complex. The GSS provides the following features to help you organize your resources:

- Locations—Logical groupings for GSS resources that correspond to geographical areas such as a city, data center, or content site

- Regions—Higher-level geographical groupings that contain one or more locations

In addition to allowing you to easily sort and navigate long lists of answers and DNS rules, the use of logical groupings such as locations and regions makes it easier to perform bulk administration of GSS resources. For example, from the primary GSSM, you can suspend or activate all answers linked to a particular GSS data center, shutting down a site for scheduled maintenance and then bringing it back online with only a few mouse clicks.

See [Chapter 2, Configuring Resources](#), for information about configuring locations and regions.

Owners

An owner is an entity that owns web content and uses the GSS to manage access to the content. As locations and regions allow you to geographically configure your GSS network, owners allow you to organizationally configure your GSS network.

For example, a service provider using the GSS to manage multiple hosting sites might create an owner for each web- or application-hosting customer. With this organizational scheme, you can associate and manage the following elements through each owner: domain lists containing that owner's hosted content, DNS rules, answer groups, and source address lists that specify how traffic to those domains should be processed.

Deployed on a corporate intranet, you can configure owners to segregate GSS resources on a department-by-department basis, or to allocate specific resources to IT personnel. For example, you can create an owner for the finance, human resources, and sales departments so that resources corresponding to each can be viewed and managed together.

See [Chapter 2, Configuring Resources](#), for information about configuring owners.

Source Addresses and Source Address Lists

A source address refers to the source of DNS queries received by the GSS. Source addresses typically point to an IP address or block of addresses that represent client D-proxies from which the queries originate.

Using a DNS rule, the GSS matches source addresses to domains hosted by the GSS using one of a number of different balance methods.

Source addresses are taken from the D-proxy (the local name server) to which a requesting client issued a recursive request. The D-proxy sends the client queries to multiple name servers, eventually querying the GSS, which matches the D-proxy source address against its list of configured source addresses.

DNS queries received by the GSS do not have to match a specific D-proxy to be routed; default routing can be performed on requests that do not emanate from a known source address. By default, the GSS provides a fail-safe “Anywhere” source address list. Incoming queries that do not match your configured source address lists are matched to this list.

Source addresses are grouped into lists, referred to as source address lists, for the purposes of routing requests. Source address lists can contain 1 to 30 source addresses or unique address blocks. Each GSS supports a maximum of 60 source address lists.

See [Chapter 3, Configuring Source Address Lists](#), for information about configuring source address lists.

Hosted Domains and Domain Lists

A hosted domain (HD) is any domain or subdomain that has been delegated to the GSS and configured using the primary GSSM for DNS query responses. A hosted domain is a DNS domain name for which the GSS is authoritative.

All DNS queries must match a domain that belongs to a configured domain list, or the GSS denies the query. Queries that do not match domains on any GSS domain lists can also be forwarded by the GSS to an external DNS name server for resolution.

Hosted domain names are limited to 128 characters. The GSS supports domain names that use wildcards. The GSS also supports POSIX 1003.2-extended regular expressions when matching wildcards.

The following examples show domain or subdomain names configured on the GSS:

```
cisco.com
www.cisco.com
www.support.cisco.com
.*\.cisco\.com
```

Domain lists are groups of hosted domains that have been delegated to the GSS. Each GSS can support a maximum of 2000 hosted domains and 2000 hosted domain lists, with a maximum of 500 hosted domains supported for each domain list.

Domain lists are used by the GSS to match incoming DNS requests to DNS rules. After the query domain is found in a domain list and matched to a DNS rule, the balance method clauses of the DNS rule define how the GSS will choose the best answer (a VIP, for example) that can service the request.

See [Chapter 4, Configuring Domain Lists](#), for information about configuring domain lists.

Answers and Answer Groups

In a GSS network, answers refer to resources to which the GSS resolves DNS requests that it receives. The three types of possible answers on a GSS network are as follows

- VIP—Virtual IP (VIP) addresses associated with an SLB such as the Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, Cisco LocalDirector, a web server, a cache, or any other geographically dispersed device in a global network deployment.
- Name Server—Configured DNS name server that can answer queries that the GSS cannot resolve.



Note

If a GSS is configured in standalone mode, a name server must be properly configured, running, and reachable in order for the GSS to successfully operate and perform DNS resolutions. If a Cisco Network Registrar (CNR) has been installed on a v2.0 GSS, however, a name server is not required.

- CRA—Content routing agents that use a resolution process called DNS race to send identical and simultaneous responses back to a user's D-proxy.

As with domains and source addresses, answers are configured using the primary GSSM by identifying the IP address to which queries can be directed.

Once created, you group answers together as resource pools called answer groups. From the available answer groups, the GSS can use a maximum of three possible response answer group and balance method clauses in a DNS rule to select the

most appropriate resource to serve a user request. Each balance method provides a different algorithm for selecting one answer from a configured answer group. Each clause specifies that a particular answer group serve the request and a specific balance method be used to select the best resource from that answer group.

Depending on the type of answer, further criteria can be applied to DNS queries to choose the best host. For example, a request that is routed to a VIP associated with a Cisco CSS is routed to the best resource based on load and availability, as determined by the CSS. A request that is routed to a content routing agent (CRA) is routed to the best resource based on proximity, as determined in a DNS race conducted by the GSS.

See [Chapter 6, Configuring Answers and Answer Groups](#), for information on configuring GSS answers and answer groups.

This section contains the following topics:

- [VIP Answers](#)
- [Name Server Answers](#)
- [CRA Answers](#)

VIP Answers

SLBs use VIP answers to represent content hosted on one or more servers under their control. The use of VIP answers enables the GSS to balance traffic among multiple origin servers, application servers, or transaction servers in a way that results in faster response times for users and less network congestion for the host.

When queried by a client's D-proxy for a domain associated with a VIP answer type, the GSS responds with the VIP address of the SLB best suited to handle that request. The requesting client then contacts the SLB, which load balances the request to the server best suited to respond to the request.

Name Server Answers

A name server answer specifies the IP address of a DNS name server to which DNS queries are forwarded from the GSS.

Using the name server forwarding feature, queries are forwarded to an external (non-GSS) name server for resolution, with the answer passed back to the GSS name server, then on to the requesting D-proxy. A name server answer can act as

a guaranteed fallback resource, a way to resolve requests that the GSS cannot resolve itself. The GSS may not be able to resolve such requests for the following reasons:

- The requested content is unknown to the GSS.
- The resources that typically handle such requests are unavailable.

The external DNS name server answer forwarded by the GSS may be able to perform the following functions:

- Use DNS server features that are not supported by the GSS, such as mail exchanger (type MX) records
- Use a third-party content provider for failover and error recovery
- Provide access to a tiered DNS system

CRA Answers

The CRA answer relies on content routing agents and the GSS to choose a suitable answer for a given query based on the proximity of two or more possible hosts to the requesting D-proxy.

With the CRA answer, requests received from a particular D-proxy are served by the content server that responds first to the request. Response time is measured using a DNS race, coordinated by the GSS and content routing agents running on each content server. In the DNS race, multiple hosts respond simultaneously to an A-record request. The server with the fastest response time (the shortest network delay between itself and the client's D-proxy) is chosen to serve the content.

The GSS requires the following information before it can initiate a DNS race:

- The delay between the GSS and each of the CRAs in each data center. With this data, the GSS computes how much time to delay the race from each data center so that each CRA starts the race simultaneously.
- The online status of the CRA through the use of keepalives.

The boomerang balance method uses the DNS race to determine the best site. See the [“DNS Race \(Boomerang\) Method”](#) section for more information on this balance method.

Keepalives

In addition to specifying a resource, each answer also provides you with the option of specifying a keepalive for that resource. A keepalive is the method by which the GSS periodically checks to determine if a resource is still active. A keepalive is a specific interaction (handshake) between the GSS and another device using a commonly supported protocol. A keepalive is designed to test if a specific protocol on the device is functioning properly. If the handshake is successful, then the device is available, active, and able to receive traffic. If the handshake fails, then the device is considered to be unavailable and inactive. All answers are validated by configured keepalives and are not returned by the GSS to the D-proxy if the keepalive indicates that the answer is not viable.

The GSS uses keepalives to collect and track information from the online status of VIPs to services and applications running on a server. You can configure a keepalive to continually monitor the online status of a resource and report that information to the primary GSSM. Routing decisions involving that resource consider the reported online status information.

The GSS also supports the use of shared keepalives to minimize traffic between the GSS and the SLBs that it is monitoring. A shared keepalive identifies a common address or resource that can provide status for multiple answers. Shared keepalives are not used with name server or CRA answers.

When configuring a VIP-type answer, you have the option to configure one of several different keepalive types or multiple keepalive types to test for that answer. The primary GSSM supports the assignment of multiple keepalives and destination ports for a specific VIP answer. You can configure a maximum of five different keepalives for a VIP answer in a mix and match configuration of ICMP, TCP, HTTP HEAD, and KAL-AP VIP keepalive types. For TCP or HTTP HEAD keepalives, you may also specify different destination ports to a VIP server.

The following sections provide additional detail about keepalives on the GSS:

- [ICMP](#)
- [TCP](#)
- [HTTP HEAD](#)
- [KAL-AP](#)
- [Scripted Keepalive](#)
- [CRA](#)

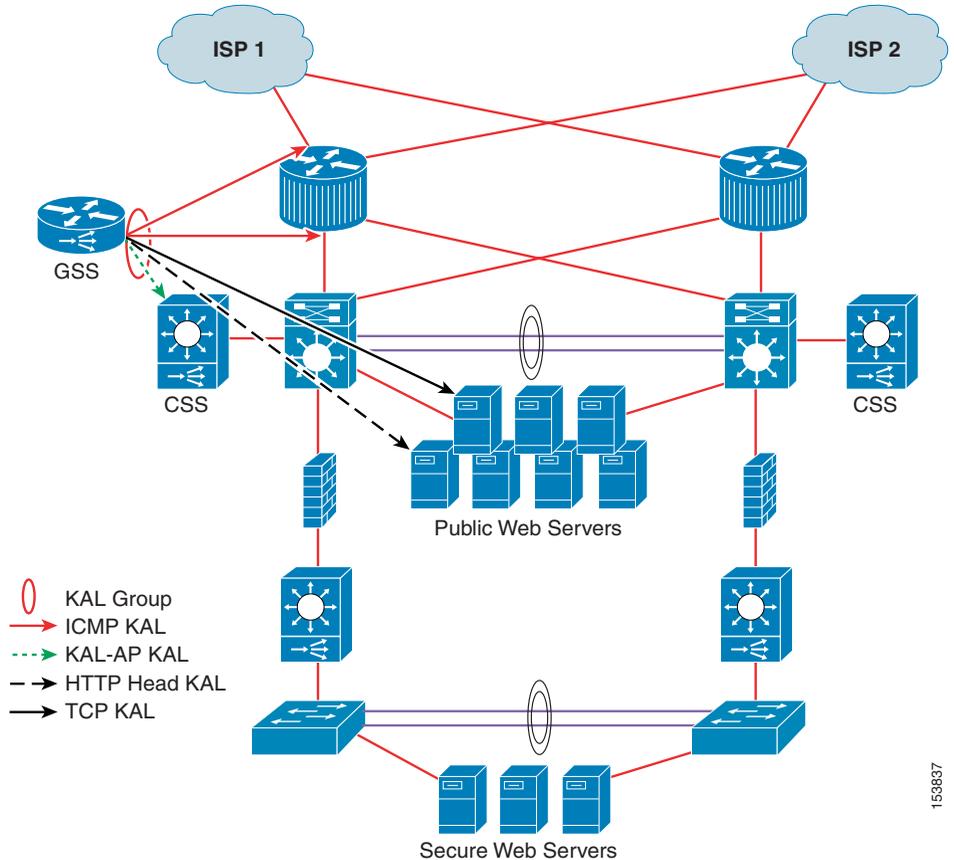
- [Name Server](#)
- [None](#)
- [Adjusting Failure Detection Time for Keepalives](#)

Multiport Keepalives

GSS supports the ability to monitor multiple devices through the use of multiport keepalives for VIP-type answers. You can configure keepalives of different types to monitor multiple ports on the VIP server. You can also configure keepalives that specify IP addresses other than that of the VIP server (for example, a router, a back-end database server, a Catalyst 6500 Series Switch, or a CSS in a data center configuration).

Multiple keepalives, each configured to probe a specified device, but acting as a group, monitor the online status of your configuration. As long as all keepalives are successful, the GSS considers the configuration active and continues to direct traffic to the data center. See [Figure 1-4](#) for a keepalive configuration example that probes multiple devices on a data center.

Figure 1-4 Using Multiple Keepalives to Monitor a Data Center



153837

**Note**

The primary GSSM allows you to configure multiple shared keepalives, as well as a single KAL-AP keepalive when specifying multiple keepalive types.

See [Chapter 5, Configuring Keepalives](#), for information about modifying global keepalive parameters and creating shared keepalives.

ICMP

Use an ICMP keepalive when testing a GSS answer that is a VIP address, IP address, or a virtual server IP address. The Internet Control Message Protocol (ICMP) keepalive type monitors the health of resources by issuing queries containing ICMP packets to the configured VIP address (or a shared keepalive address) for the answer. Online status is determined by a response from the targeted address, indicating simple connectivity to the network. The GSS supports a maximum of 750 ICMP keepalives when using the standard detection method and a maximum of 150 ICMP keepalives when using the fast detection method. See the [“Adjusting Failure Detection Time for Keepalives”](#) section for details.

TCP

Use a TCP keepalive when testing a GSS answer that is a GSLB device that may be something other than a CSS or CSM. GSLB remote devices may include webservers, LocalDirectors, Wireless Application Protocol (WAP) gateways, and other devices that can be checked using a TCP keepalive. The TCP keepalive initiates a TCP connection to the remote device by performing the three-way handshake sequence.

Once the TCP connection is established, the GSS terminates the connection. You can choose to terminate the connection from two termination methods: Reset (immediate termination using a hard reset) or Graceful (standard three-way handshake termination).

The GSS supports a maximum of 1500 TCP keepalives when using the standard detection method and a maximum of 150 TCP keepalives when using the fast detection method. See the [“Adjusting Failure Detection Time for Keepalives”](#) section for details.

HTTP HEAD

Use an HTTP HEAD keepalive when testing a GSS answer that is an HTTP web server acting as a standalone device or managed by an SLB device such as a Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, or Cisco LocalDirector. The HTTP HEAD keepalive type sends a TCP-formatted HTTP HEAD request to a web server at an address that you specify. The online status of the device is returned in the form of an HTTP Response Status Code of 200 (for example, HTTP/1.0 200 OK).

Once the HTTP HEAD connection is established, the GSS terminates the connection. There are two methods to terminate the connection: Reset (immediate termination using a hard reset) or Graceful (standard three-way handshake termination).

The GSS supports a maximum of 500 HTTP HEAD keepalives when using the standard detection method and a maximum of 100 HTTP HEAD keepalives when using the fast detection method. See the [“Adjusting Failure Detection Time for Keepalives”](#) section for details.

KAL-AP

Use a KeepAlive-Appliance Protocol (KAL-AP) keepalive when testing a GSS answer that is a VIP associated with a Cisco CSS or a Cisco CSM. The KAL-AP keepalive type sends a detailed query to both a primary (master) and an optional secondary (backup) circuit address that you specify. The online status and load of each VIP that is specified in the KAL-AP keepalive are returned.

Depending on your GSS network configuration, you can use the KAL-AP keepalive to either query a VIP address directly (KAL-AP By VIP) or query an address with an alphanumeric tag (KAL-AP By Tag). Using a KAL-AP By Tag keepalive query can be useful in the following cases:

- You are attempting to determine the online status of a device that is located behind a firewall that is performing Network Address Translation (NAT).
- There are multiple content rule choices on the SLB.

The GSS supports a maximum of 128 primary and 128 secondary KAL-AP keepalives when using the standard detection method and a maximum of 40 primary and 40 secondary KAL-AP keepalives when using the fast detection method. See the [“Adjusting Failure Detection Time for Keepalives”](#) section for details.

Scripted Keepalive

Use a Scripted keepalive when you wish to probe third-party devices and obtain the load information. The Scripted keepalive uses the SNMP get request to fetch the load information from the target device.

**Note**

A Scripted keepalive must always be a shared keepalive.

The GSS supports a maximum of 384 Scripted keepalives when using the standard detection method and 120 Scripted keepalives when using the fast detection method. See the [“Adjusting Failure Detection Time for Keepalives”](#) section for details. Secondary Scripted keepalives are not supported in the GSS.

CRA

Use the CRA keepalive when testing a CRA answer that responds to DNS race requests. The CRA keepalive type tracks the time required (in milliseconds) for a packet of information to reach the CRA and return to the GSS. The GSS supports a maximum of 200 CRA keepalives.

Name Server

Use the name server keepalive to send a query to the IP address of the name server for a specified query domain (for example, www.cisco.com). The online status for the name server answer is determined by the ability of the name server for the query domain to respond to the query and assign the domain to an address. The GSS supports a maximum of 100 name server keepalives.

None

With the keepalive set to None, the GSS assumes that the answer is always online. Setting the keepalive type to None prevents your GSS from taking online status or load into account when routing. However, a keepalive of None can be useful under certain conditions, such as when adding devices to your GSS network that are not suited to other keepalive types. ICMP is a simple and flexible keepalive type that works with most devices. Using ICMP is often preferable to using the None option.

Adjusting Failure Detection Time for Keepalives

Failure detection time, for the GSS, is the amount of time between when a device fails (the answer resource goes offline) and when the GSS realizes the failure occurred. If a response packet fails to arrive back to the GSS within this window, the answer is marked offline.

The GSS supports two failure detection modes: standard and fast.

With standard mode, the failure detection time is typically 60 seconds before the GSS detects that a failure has occurred. Standard mode allows adjustment of the following parameters:

- **Response Timeout**—Length of time allowed before the GSS retransmits data to a device that is not responding to a request. The valid entries are 20 to 60 seconds. The default is 20 seconds.
- **Minimum Interval**—Minimum interval with which the GSS attempts to schedule a keepalive. The valid entries are 40 to 255 seconds. The default is 40 seconds.

With fast mode, the GSS controls the failure detection time by using the following keepalive transmission interval formula:

$$(\# \text{ Ack'd Packets} * (\text{Response TO} + (\text{Retry TO} * \# \text{ of Retries}))) + \text{Timed Wait}$$

where:

Ack'd Packets = Number of packets that require some form of acknowledgement

Response TO = Response Timeout, which is the length of time to wait for a reply for a packet that requires an acknowledgement

Retry TO = Retry Timeout, which is the length of time to wait for a reply for a retransmitted packet

of Retries = Number of Retries, which is the number of times the GSS retransmits packets to a potentially failed device before declaring the device offline

Timed Wait = Time for the remote side of the connection to close (TCP-based keepalive only)

Table 1-1 summarizes how the GSS calculates the fast keepalive transmission rates for a single keepalive per answer.

Table 1-1 Keepalive Transmission Rates for a Single Keepalive Per Answer

	# Ack'd Packets (Fixed Value)	Response TO (Fixed Value)	Retry TO (Fixed Value)	# of Retries (User Selectable)	Timed Wait (Fixed Value)	Transmission Interval
KAL-AP	1	2 seconds	2 seconds	1	0	4 seconds
ICMP	1	2 seconds	2 seconds	1	0	4 seconds

Table 1-1 *Keepalive Transmission Rates for a Single Keepalive Per Answer*

	# Ack'd Packets (Fixed Value)	Response TO (Fixed Value)	Retry TO (Fixed Value)	# of Retries (User Selectable)	Timed Wait (Fixed Value)	Transmission Interval
TCP (RST)	1	2 seconds	2 seconds	1	0	4 seconds
TCP (FIN)	2	2 seconds	1 second	1	2 seconds	10 seconds
HTTP HEAD (RST)	2	2 seconds	2 seconds	1	0	8 seconds
HTTP HEAD (FIN)	3	2 seconds	2 seconds	1	2 seconds	14 seconds

For a TCP (RST) connection, the default transmission interval for a TCP keepalive is as follows:

$$(1 * (2 + (2 * 1))) + 0 = 4 \text{ seconds}$$

You can adjust the number of retries for the ICMP, TCP, HTTP HEAD, and KAL-AP keepalive types. The number of retries defines the number of times that the GSS retransmits packets to a potentially failed device before declaring the device offline. The GSS supports a maximum of 10 retries, with a default of 1. As you adjust the number of retries, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries decreases the detection time.

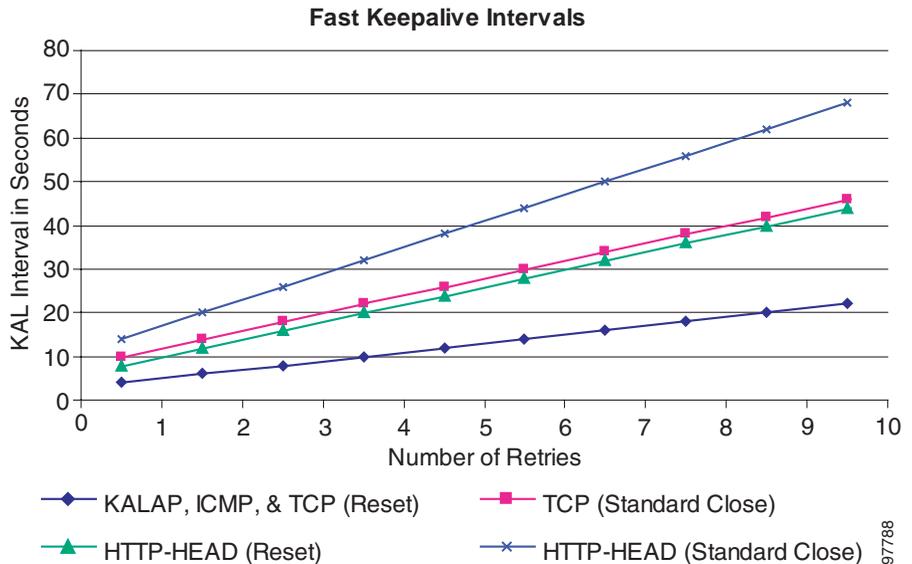
The GSS associates the number of retries value with every packet that requires some form of acknowledgement before continuing with a keepalive cycle (ICMP requests, TCP SYN, or TCP FIN). For example, to fully complete a TCP-based keepalive cycle, the TCP-based keepalive retries the SYN packet for the specified number of retries and then retries the FIN packet for the specified number of retries.

In the above example of a TCP (RST) connection, if you change the number of retries from the default value of 1 to a setting of 5, the transmission interval would be as follows:

$$(1 * (2 + (2 * 5))) + 0 = 12 \text{ seconds}$$

[Figure 1-5](#) shows the effect on the keepalive transmission interval as you increase the number of retries value.

Figure 1-5 Effect of the Number of Retries Value on the Keepalive Transmission Interval



You can also define the number of consecutive successful keepalive attempts (probes) that must occur before the GSS identifies that an offline answer is online. The GSS monitors each keepalive attempt to determine if the attempt was successful. The **successful-probes** keyword identifies how many consecutive successful keepalive attempts the GSS must recognize before bringing an answer back online and reintroducing it back into the GSS network.

The primary GSSM allows you to assign multiple keepalives for a single VIP answer. You can configure a maximum of five different keepalives for a VIP answer in a mix and match configuration of ICMP, TCP, HTTP HEAD, and KAL-AP VIP keepalive types. In this configuration, the failure detection times are based on the calculated transmission levels identified for each of the different keepalives associated with an answer.

Balance Methods

The GSS supports six unique balance methods that allow you to specify how a GSS answer should be selected to respond to a given DNS query. Each balance method provides a different algorithm for selecting one answer from a configured answer group. This section explains the balance methods supported by the GSS and includes the following topics:

- [Ordered List Method](#)
- [Round-Robin Method](#)
- [Weighted Round-Robin Method](#)
- [Least-Loaded Method](#)
- [Hashed Method](#)
- [DNS Race \(Boomerang\) Method](#)

Ordered List Method

When the GSS uses the ordered list balance method, each resource within an answer group (for example, an SLB VIP or a name server) is assigned a number that corresponds to the rank of that answer within the group. The number you assign represents the order of the answer on the list. Subsequent VIPs or name servers on the list are only used if preceding VIPs or name servers on the list are unavailable. The GSS supports gaps in numbering in an ordered list.

**Note**

For answers that have the same order number in an answer group, the GSS uses only the first answer that contains the number. You should specify a unique order number for each answer in an answer group.

Using the ranking of each answer, the GSS tries each resource in the order that has been assigned, selecting the first available live answer to serve a user request. List members are given precedence and tried in order, and a member is not used unless all previous members fail to provide a suitable result.

The ordered list method allows you to manage resources across multiple content sites in which a deterministic method for selecting answers is required.

See the [“Balance Method Options for Answer Groups”](#) section for information about how the GSS determines which answer to select when using the ordered list balance method.

Round-Robin Method

When the GSS uses the round-robin balance method, each resource within an answer group is tried in turn. The GSS cycles through the list of answers, selecting the next answer in line for each request. In this way, the GSS can resolve requests by evenly distributing the load among possible answers.

The round-robin balance method is useful when balancing requests among multiple, active data centers that are hosting identical content; for example, between SLBs at a primary and at an active standby site that serves requests.

See the [“Balance Method Options for Answer Groups”](#) section for information about how the GSS determines which answer to select when using the round-robin balance method.

Weighted Round-Robin Method

As performed by the round-robin balance method, the weighted round-robin method also cycles through a list of defined answers to choose each available answer in turn. However, with weighted round-robin, an additional weight factor is assigned to each answer, biasing the GSS toward certain servers so that they are used more often.

See the [“Balance Method Options for Answer Groups”](#) section for information about how the GSS determines which answer to select when using the weighted round-robin balance method.

Least-Loaded Method

When the GSS uses the least-loaded balance method, the GSS resolves requests to the least loaded of all resources, as reported by the KAL-AP keepalive process, which provides the GSS with detailed information on the SLB load and availability.

The least-loaded balance method resolves the request by determining the least number of connections on a CSM or the least-loaded CSS.

See the “[Balance Method Options for Answer Groups](#)” section for information about how the GSS determines which answer to select when using the least-loaded balance method.

Hashed Method

When the GSS uses the hashed balance method, elements of the client’s DNS proxy IP address and the requesting client’s domain are extracted to create a unique value, referred to as a hash value. The unique hash value is attached to and used to identify a VIP that is chosen to serve the DNS query.

The use of hash values makes it possible to stick traffic from a particular requesting client to a specific VIP, ensuring that future requests from that client are routed to the same VIP. This type of continuity can be used to facilitate features, such as online shopping baskets, in which client-specific data is expected to persist even when client connectivity to a site is terminated or interrupted.

The GSS supports the following two hashed balance methods. You can apply one or both hashed balance methods to the specified answer group:

- **By Source Address**—The GSS selects the answer based on a hash value created from the source address of the request.
- **By Domain Name**—The GSS selects the answer based on a hash value created from the requested domain name.

DNS Race (Boomerang) Method

The GSS supports the DNS race (boomerang) method of proximity routing, which is a type of DNS resolution initiated by the GSS to load balance 2 to 20 sites.

The boomerang method is based on the concept that instantaneous proximity can be determined if a CRA within each data center sends an A-record (IP address) at the exact same time to the client’s D-proxy. The DNS race method of DNS resolution gives all CRAs (Cisco content engines or content services switches) a chance at resolving a client request and allows for proximity to be determined without probing the client’s D-proxy. The first A-record received by the D-proxy is, by default, considered to be the most proximate.

For the GSS to initiate a DNS race, it needs to establish the following information for each CRA:

- The delay between the GSS and each of the CRAs in each data center. With this data, the GSS computes the length of time to delay the race from each data center, so that each CRA starts the race simultaneously.
- The online status of the CRAs. With this data, the GSS knows not to forward requests to any CRA that is not responding.

The boomerang server on the GSS gathers this information by sending keepalive messages at predetermined intervals. The boomerang server uses this data, along with the IP addresses of the CRAs, to request the exact start time of the DNS race.

If the CRA response is to be accepted by the D-proxy, each CRA must spoof the IP address of the GSS to which the original DNS request was sent.

Balance Method Options for Answer Groups

For most balance methods supported by the GSS, there are additional configuration options when you group specific answers in an answer group. These configuration options ensure the GSS properly applies the balance method for answers, and that you receive the best possible results from your GSS device.

[Table 1-2](#) describes the available answer group options for each answer type (VIP, CRA, or NS) and balance method combination.

Table 1-2 Answer Group Options

Answer Type	Balance Methods Used	Answer Group Options
VIP	Hashed Least-loaded Ordered list Round-robin Weighted round-robin	Order Load threshold Weight

Table 1-2 Answer Group Options (continued)

Answer Type	Balance Methods Used	Answer Group Options
Name server	Hashed Ordered list Round-robin Weighted round-robin	Order Weight
CRA	Boomerang (DNS race)	None

This section explains each of the options available for the answers in an answer group. It contains the following topics:

- [Order](#)
- [Weight](#)
- [Load Threshold](#)

Order

Use the Order option when the balance method for the answer group is Ordered List. Answers on the list are given precedence based upon their position in the list in responding to requests.

Weight

Use the answer group Weight option when the balance method for the answer group is weighted round-robin or least-loaded. You specify a weight by entering a value from 1 and 10. This value indicates the capacity of the answer to respond to requests. The weight creates a ratio that the GSS uses when directing requests to each answer. For example, if Answer A has a weight of 10 and Answer B has a weight of 1, Answer A receives 10 requests for every 1 request directed to Answer B.

When you specify a weight for the weighted round-robin balance method, the GSS creates a ratio of the number of times that the answer is used to respond to a request before trying the next answer on the list.

When you specify a weight for the least-loaded balance method, the GSS uses that value as the divisor for calculating the load number associated with the answer. The load number creates a bias in favor of answers with a greater capacity.

Load Threshold

Use the Load Threshold option when the answer type is VIP and the keepalive method is KAL-AP to determine whether an answer is available, regardless of the balance method used. The load threshold is a number from 2 and 254 that is compared to the load being reported by the answer device. If the reported load is greater than the specified threshold, the answer is considered offline and unavailable to serve further requests.

Traffic Management Load Balancing

The GSS includes DNS sticky and network proximity traffic management functions to provide advanced global server load-balancing capabilities in a GSS network.

DNS sticky ensures that e-commerce sites provide uninterrupted services and remain open for business by supporting persistent sticky network connections between customers and e-commerce servers. Persistent network connections ensure that active connections are not interrupted and shopping carts are not lost before purchase transactions are completed.

Network proximity selects the closest or most proximate server based on measurements of round-trip time to the requesting client's D-proxy location, improving the efficiency within a GSS network. The proximity calculation is typically identical for all requests from a given location (D-proxy) if the network topology remains constant. This approach selects the best server based on a combination of site health (availability and load) and the network distance between a client and a server zone.

This section contains the following topics:

- [DNS Sticky GSLB](#)
- [Network Proximity GSLB](#)

DNS Sticky GSLB

Stickiness, also known as persistent answers or answer caching, enables a GSS to remember the DNS response returned for a client D-proxy and to later return that same answer when the client D-proxy makes the same request. When you enable stickiness in a DNS rule, the GSS makes a best effort to always provide identical A-record responses to the requesting client D-proxy, assuming that the original VIP continues to be available.

DNS sticky on a GSS ensures that e-commerce clients remain connected to a particular server for the duration of a transaction even when the client's browser refreshes the DNS mapping. While some browsers allow client connections to remain for the lifetime of the browser instance or for several hours, other browsers impose a connection limit of 30 minutes before requiring a DNS re-resolution. This time may not be long enough for a client to complete an e-commerce transaction.

With local DNS sticky, each GSS device attempts to ensure that subsequent client D-proxy requests to the same domain name to the same GSS device will be stuck to the same location as the first request. DNS sticky guarantees that all requests from a client D-proxy to a particular hosted domain or domain list are given the same answer by the GSS for the duration of a user-configurable sticky inactivity time interval, assuming the answer is still valid.

With global DNS sticky enabled, each GSS device in the network shares answers with the other GSS devices in the network, operating as a fully connected peer-to-peer mesh. Each GSS device in the mesh stores the requests and responses from client D-proxies in its own local database and shares this information with the other GSS devices in the network. As a result, subsequent client D-proxy requests to the same domain name to any GSS in the network causes the client to be stuck.

The DNS sticky selection process is initiated as part of the DNS rule balance method clause.

See [Chapter 8, Configuring DNS Sticky](#) for information about configuring local and global DNS sticky for GSS devices in your network.

Network Proximity GSLB

The GSS responds to DNS requests with the most proximate answers (resources) relative to the requesting D-proxy. In this context, proximity refers to the distance or delay in terms of network topology (not geographical distance) between the requesting client's D-proxy and its answer.

To determine the most proximate answer, the GSS communicates with a probing device, a Cisco IOS-based router, located in each proximity zone to gather round-trip time (RTT) metric information measured between the requesting client's D-proxy and the zone. Each GSS directs client requests to an available server with the lowest RTT value.

The proximity selection process is initiated as part of the DNS rule balance method clause. When a request matches the DNS rule and balance clause with proximity enabled, the GSS responds with the most proximate answer.

See [Chapter 9, Configuring Network Proximity](#) for information about configuring proximity for GSS devices in your network.

DDoS Detection and Mitigation

Distributed Denial of Service (DDoS) attacks are designed to deny legitimate users access to a specific computer or network resources. These attacks are originated by malicious attackers who send several thousand spoofed DNS requests to a target device. The target then treats these requests as valid and returns the DNS replies to the spoofed recipient (that is, the victim).

Since the target is busy replying to the attackers, it drops valid DNS requests from legitimate D-proxies. When the number of requests is in the thousands, the attacker can potentially generate a multi-gigabit flood of DNS replies, thus causing network congestion.

In such cases, the following network points are affected:

- The performance of the target device is degraded because it is busy processing spoofed requests.
- The traffic generated by the replies traverses the internet backbone affecting the ISP and any upstream providers.
- A host with an IP address similar to the one used in the spoofing operation receives large amounts of inbound DNS traffic.

To combat such problems, the GSS contains a licensed DDoS detection and mitigation module. For more information about obtaining and installing a DDoS license, see the *Global Site Selector Administration Guide*.

Typically, the DDoS module prevents the following:

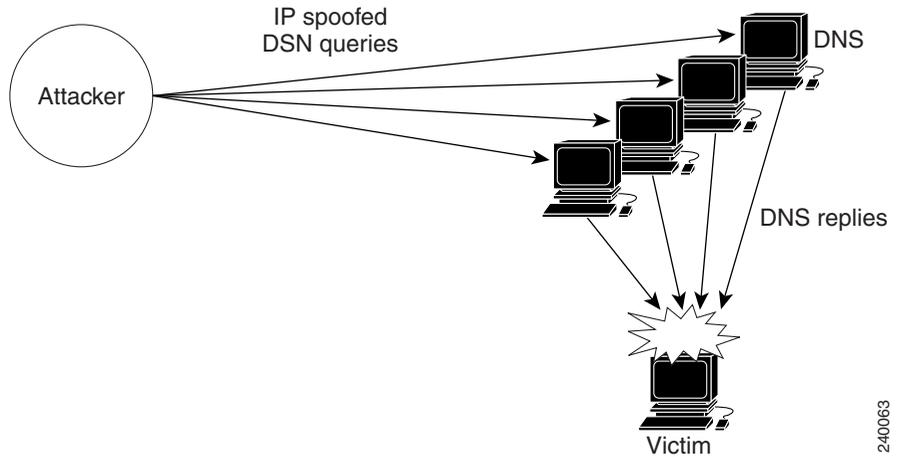
- Reflector attacks where the attacker spoofs the IP address of the victim (that is, the GSS). See the “[Mitigation Rules](#)” section for more information.
- Attacks where malformed DNS packets are transmitted
- Attacks where DNS queries are sent:
 - For any domain (that is, a DoS replay attack) from a specific source IP.
 - For domains not configured on the GSS
 - From different source IPs globally exceeding the GSS packet processing rate.
 - From spoofed IP addresses

The DDoS module prevents these attacks by performing three primary functions, each of which is explained in the sections that follow:

- [Mitigation Rules](#)
- [Rate Limits](#)
- [Anti-Spoofing Mechanism](#)

Mitigation Rules

A reflector attack occurs when the attacker spoofs the IP address of the victim (in this case, the GSS) and sends multiple DNS requests to a DNS server or multiple DNS servers posing as the victim (see [Figure 1-6](#)). The amplification effect is based on the fact that small queries can generate larger UDP packets in response and bombard the victim with a high-volume of DNS response traffic.

Figure 1-6 Reflector Attack Diagram

240063

The following GSS basic mitigation rules help reduce the reflector problem:

- Packets are dropped with a source port other than 53 and a QR bit of 1 (response) when responses come from a source port other than 53.
- Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.
- Packets are dropped with a source port equal to 53, but less than 1024, and a QR bit of 0 (request).

By default, mitigation rules are enabled. For more information on enabling mitigation, see [Chapter 10, Configuring DDoS Prevention](#).

Rate Limits

The GSS enforces a limit on the number of DNS packets per second for each individual D-proxy, or an overall global rate limit. It does not enforce a limit for all other traffic. Initially, this limit is the default value. However, you can adjust the limit during peacetime, or overwrite it by configuring either a D-proxy or a group of D-proxies. Once this limit is exceeded, DNS packets are dropped.

**Note**

The final rate limits for each D-proxy and the global rate limit are determined by multiplying the rate limits learned during peacetime (or configured via the CLI) with a tolerance factor. You can configure this value by using the **rate-limit global** and **tolerance-factor global** CLI commands in `ddos` configuration mode. For more details, see [Chapter 10, Configuring DDoS Prevention](#).

Anti-Spoofing Mechanism

Spoofed packets contain an IP address in the header that is not the actual IP address of the originating device. Spoofed attacks aim to saturate the target site links and the target site server resources or zone. The source IP addresses of the spoofed packets can be random, or have specific, focused addresses.

Spoofed attacks can be generated easily in a high volume, even from a single device because they cannot be stopped using access lists (ACLs) or filters. The reason is that the attacker can continuously change the source IP address of the packets.

To overcome spoofed attacks, the GSS uses an anti-spoofing mechanism called Redirect to TCP. This mechanism is used for DNS queries and is also called DNS-proxy. It is based on forcing the client to resend its query using TCP. Once the query arrives in TCP, the GSS uses a challenge/response mechanism to authenticate the source. If the source succeeds with authentication, the GSS sends a TCP reply back. The D-proxy sends a UDP request, while the GSS sends a TC or truncated bit. The D-proxy returns on TCP and the GSS then sends the reply on TCP.

**Note**

GSS provides anti-spoofing for all request packets (identified by `qrbit=0`), with the exception of TSIG, DDNS (`opcode=5`) and DNS notify (`opcode=4`) requests.

The challenge-response algorithms work by distinguishing spoofed traffic from non-spoofed traffic. The GSS sends a challenge, also known as a cookie, to a client that tries to connect to the GSS. If the source IP address in the packet header is the IP address that is assigned to the client, the client receives the challenge and sends back a response.

If the source IP address in the packet is spoofed, however, the client that generated the original traffic to the zone does not receive the GSS response and thus, does not answer with the correct challenge. The GSS considers clients as authenticated only when they return correct challenges. The DDoS module only allows traffic from such clients to pass on to the selector or the Cisco Network Registrar (CNR).

See [Chapter 10, Configuring DDoS Prevention](#) for specific instructions about enabling DDoS and configuring filters, rate limits, and anti-spoofing mechanisms.

GSS Network Deployment

A typical GSS deployment may contain a maximum of eight GSS devices deployed on a corporate intranet or the Internet. At least one GSS must be configured as a primary GSSM. Optionally, a second GSS can be configured as a standby GSSM. The primary GSSM monitors the other GSS devices on the network and offers features for managing and monitoring request routing services using CLI commands or a GUI accessible through secure HTTP. Only one GSSM can be active at any time, with the second GSSM serving as a standby, or backup device.

The GSSM functionality is embedded on each GSS, and any GSS device can be configured to act as a primary GSSM or a standby GSSM.

You can configure additional GSS devices on the GSS network to respond to DNS requests and transmit periodic keepalives to provide resource state information about devices. The GSS devices do not perform primary GSSM network management tasks.

This section describes a typical network deployment of the GSS and contains the following topics:

- [Locating GSS Devices](#)
- [Locating GSS Devices Behind Firewalls](#)
- [Communication Between GSS Nodes](#)
- [Deployment Within Data Centers](#)

Locating GSS Devices

Although your organization determines where your GSS devices are deployed in your network, you should follow these guidelines when deploying these devices.

Because the GSS serves as the authoritative name server for one or more domains, each GSS must be publicly or privately addressable on your enterprise network to allow the D-proxy clients requesting content to find the GSSs assigned to handle DNS requests.

Options are available for delegating responsibility for your domain to your GSS devices, depending on traffic patterns to and from your domain. For example, given a network containing five GSS devices, you might choose to modify your parent domain DNS servers so that all traffic sent to your domain is directed to your GSS network. You may also choose to have a subset of your traffic delegated to one or more of your GSSs, with other devices handling other segments of your traffic.

See [Chapter 7, Building and Modifying DNS Rules](#) for information about modifying your network DNS configuration to accommodate the addition of GSS devices to your network.

Locating GSS Devices Behind Firewalls

Deploying a firewall can prevent unauthorized access to your GSS network and eliminate common denial of service (DoS) attacks on your GSS devices. In addition to being deployed behind your corporate firewall, the GSS packet-filtering features can enable GSS administrators to permit and deny traffic to any GSS device.

When positioning your GSS behind a firewall or enabling packet filtering on the GSS itself, you must properly configure each device (the firewall and the GSS) to allow valid network traffic to reach the GSS device on specific ports. In addition to requiring HTTPS traffic to access the primary GSS graphical user interface, you may want to configure your GSSs to allow FTP, Telnet, and SSH access through certain ports. In addition, GSSs must be able to communicate their status to and receive configuration information from the GSSM. Also, primary and standby GSSMs must be able to communicate and synchronize with one another. Finally, if global DNS sticky is enabled on the GSS network, all GSSs in the sticky mesh must be able to communicate with each other to share the sticky database.

See the *Cisco Global Site Selector Administration Guide* for information about access lists to limit incoming traffic. See the “Deploying GSS Devices Behind Firewalls” section for information on which ports must be enabled and left open for the GSS to function properly.

Communication Between GSS Nodes

All GSS devices, including the primary GSSM and standby GSSM, respond to DNS queries and perform keepalives to provide global server load-balancing. Additionally, the primary GSSM acts as the central management device and hosts the embedded GSS database that contains shared configuration information, such as DNS rules, for each GSS that it controls. Use the primary GSSM to make configuration changes, which are automatically communicated to each registered GSS device that the primary GSSM manages.

The standby GSSM performs GSLB functions for the GSS network. The standby GSSM can act as the interim primary GSSM for the GSS network if the designated primary GSSM suddenly goes offline or becomes unavailable to communicate with other GSS devices. If the primary GSS goes offline, the GSS network continues to function and does not impact global server load balancing.

The GSS performs routing of DNS queries based on the DNS rules and conditions created from the primary GSSM. Each GSS device on the network delegates authority to the parent domain GSS DNS server that serves the DNS requests.

Each GSS is known to and synchronized with the primary GSSM. Unless global DNS sticky is enabled, individual GSSs do not report their presence or status to one another. If a GSS unexpectedly goes offline, the other GSSs on the network that are responsible for the same resources remain unaffected.

With both a primary and a standby GSSM deployed on your GSS network, device configuration information and DNS rules are automatically synchronized between the primary GSSM and a data store maintained on the standby GSSM.

Synchronization occurs automatically between the two devices whenever the GSS network configuration changes. Updates are packaged and sent to the standby GSSM using a secure connection between the two devices.

See the *Cisco Global Site Selector Administration Guide* for instructions on enabling each GSS device in the GSS network and for details about changing the GSSM role in the GSS network.

Deployment Within Data Centers

A typical GSS network consists of multiple content sites, such as data centers and server farms. Access to a data center or server farm is managed by one or more SLBs, such as the Cisco CSS or Cisco CSM. One or more virtual IP addresses (VIPs) represent each SLB. Each VIP acts as the publicly addressable front end of the data center. Behind each SLB are transaction servers, database servers, and mirrored origin servers offering a wide variety of content, from websites to applications.

The GSS communicates directly with the SLBs representing each data center by collecting statistics on availability and load for each SLB and VIP. The GSS uses the data to direct requests to the most optimum data centers and the most available resources within each data center.

In addition to SLBs, a typical data center deployment may also contain DNS name servers that are not managed by the GSS. These DNS name servers can resolve requests through name server forwarding that the GSS is unable to resolve.

GSS Network Management

Management of your GSS network is divided into two types:

- [CLI-Based GSS Management](#)
- [GUI-Based Primary GSSM Management](#)

Certain GSS network management tasks require that you use the CLI (initial device setup, sticky and proximity group configuration, for example). Other tasks require that you use the GUI (User Views and Roles, for example). In most cases, you have the option of using either the CLI or the GUI at the primary GSSM to perform GSLB configuration and monitoring.

Choosing when to use the CLI and when to use the GUI are also a matter of personal or organizational choice. Additionally, you can create your GSLB configuration using one method and then modify it using the alternate method.

This configuration guide describes how to use the CLI to perform global server load balancing. In cases where you must use the GUI to perform a particular task (configuring DNS rule filters, for example), the task is listed and a reference to the appropriate chapter in the *Global Site Selector GUI-Based Global Load-Balancing Configuration Guide* is provided.

CLI-Based GSS Management

You can use the CLI to configure the following installation, management, and global server load-balancing tasks for your GSS:

- Initial setup and configuration of GSS and GSSM (primary and standby) devices
- Software upgrades and downgrades on GSSs and GSSMs
- Database backups, configuration backups, and database restore operations
- Global server load balancing configuration and DNS request handling by creating DNS rules and monitoring keepalives at the primary GSSM

In addition, you can use the CLI for the following network configuration tasks:

- Network address and hostname configuration
- Network interface configuration
- Access control for your GSS devices, including IP filtering and traffic segmentation

You can also use the CLI for local status monitoring and logging for each GSS device.

See the *Cisco Global Site Selector Command Reference* for an alphabetical list of all GSS CLI commands including syntax, options, and related commands.

GUI-Based Primary GSSM Management

The primary GSSM offers a single, centralized graphical user interface (GUI) for monitoring and administering your entire GSS network. You can use the primary GSSM GUI to perform the following tasks:

- Configure DNS request handling and global server load balancing by creating DNS rules and monitoring keepalives
- Activate GSSs that are configured on the GSS network
- Monitor GSS network resources
- Monitor request routing and GSS statistics

For more information about the GUI, see the *Global Site Selector GUI-Based Global Load-Balancing Configuration Guide*.

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 are ready to begin configuring request routing and global server load balancing for your GSS network. See the *Cisco Global Site Selector Getting Started Guide* for procedures on getting your GSSM (primary and standby) and GSS devices set up, configured, and ready to perform global server load balancing.

Use CLI commands or the GUI on the primary GSSM to configure global server load balancing for your GSS network. You configure keepalives to monitor the health of SLBs and servers on your network, and you create and manage DNS rules and the associated global server load-balancing configuration to process incoming DNS requests.

To configure your GSS devices and resources from the primary GSSM for global server load balancing, perform the following steps:

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

2. Create one or more source address lists—Optional. Use these lists of IP addresses to identify the name servers (D-proxy) that forward requests for the specified domains. The default source address list is Anywhere to match any incoming DNS request to the domains. See [Chapter 3, Configuring Source Address Lists](#), for details.
3. Create one or more domain lists—Establish lists of Internet domains, possibly using wildcards, that are managed by the GSS and queried by users. See [Chapter 4, Configuring Domain Lists](#), for details.
4. Modify the default global keepalive settings or create any shared keepalives—Optional. The GSS regularly polls to monitor the online status of one or more GSS resources linked to the keepalive. Shared keepalives are required for any answer that uses the KAL-AP keepalive type. See [Chapter 5, Configuring Keepalives](#), for details.
5. Create one or more answers and answer groups—Answers are resources that match requests to domains. Answer groups are collections of resources that balance requests for content. See [Chapter 6, Configuring Answers and Answer Groups](#), for details.
6. Build the DNS rules that will control global server load balancing on your GSS network. See [Chapter 7, Building and Modifying DNS Rules](#), for details.
7. If you plan to use DNS sticky for your global server load balancing, configure local or global DNS sticky for GSS devices in your network —Stickiness enables the GSS to remember the DNS response returned for a client D-proxy and to later return that answer when the client makes the same request. See [Chapter 8, Configuring DNS Sticky](#), for details.
8. If you plan to use network proximity for your global server load balancing, configure proximity for GSS devices in your network—Proximity determines the best (most proximate) resource for handling global load-balancing requests. See [Chapter 9, Configuring Network Proximity](#), for details.
9. If you plan to use the GSLB configuration file functionality, create, modify, and execute GSLB configuration files to automate the global server load-balancing process for your network. See [Chapter 11, Creating and Playing GSLB Configuration Files](#), for details.

Where to Go Next

[Chapter 2, Configuring Resources](#) describes how to organize resources on your GSS network as locations, regions, and owners.



CHAPTER 2

Configuring Resources

This chapter describes how to establish global server load-balancing resources on your GSS network.

This chapter contains the following major sections:

- [Organizing Your GSS Network](#)
- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Configuring Locations and Regions](#)
- [Configuring Owners](#)
- [Grouping GSS Resources by Location, Region, and Owner](#)
- [Displaying Resource Information](#)
- [Where to Go Next](#)

Organizing Your GSS Network

The primary GSSM provides you with the following means to group and organize resources on your GSS network:

- **Locations**—Logical groupings for GSS resources that correspond to geographical entities such as a city, data center, or content site
- **Regions**—Higher-level geographical groupings that contain one or more locations
- **Owners**—Groupings that correspond to business or organizational relationships; for example, customers, internal departments, and IT personnel

Regions and locations do not have to correspond to actual geographical sites; they are simply organizing measures that allow you to group GSS resources and exist in a relationship of one (region) to many (locations).

In addition to providing an organizational scheme for your GSS network, locations can also be used for bulk management of GSS resources, such as answers. Answers can be grouped and managed according to an established GSS location. Using a location to manage your answers can simplify the process to suspend or activate answers in a particular area of your network (see [Chapter 6, Configuring Answers and Answer Groups](#)). For example, you can shut down one or more data centers to perform software upgrades or regular maintenance.

Before you can configure your GSS network resources, you must log in to the CLI and enable privileged EXEC mode. See the [“Logging in to the CLI and Enabling Privileged EXEC Mode”](#) section for details.

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Configuring Locations and Regions

This section contains the following topics:

- [Configuring Regions](#)
- [Configuring Locations](#)



Note

We recommend that you create regions before you create locations because you associate a region with a location when creating the location.

Configuring Regions

You configure a region by using the **region** command in global server load-balancing configuration mode.

The syntax for this command is as follows:

```
region name [comments text]
```

The keywords and arguments for this command are as follows:

- *name*—A high-level geographical group name for the region assigned to the GSS network. Enter a unique alphanumeric name with a maximum of 80 characters. Enter names that include spaces in quotes (for example, “name 1”).
- **comments** *text*—(Optional) Specifies descriptive information or important notes about the region. Enter a maximum of 256 alphanumeric characters. Comments with spaces must be entered in quotes.

For example, to create a region named `Western_EU` and provide comments about its location and purpose, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# region Western_EU comments "London and
future data centers"
```

If you need to delete a region, ensure that you know about the dependencies associated with it. For example, regions that have locations associated with them cannot be deleted. In this case, you must first delete any associated locations.

**Caution**

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

If an error appears informing you that a GSS location is still linked to the region that you want to delete, change the region associated with the location, and then attempt to delete the region again.

To delete a region, enter:

```
gssm1.example.com(config-gslb)# no region Western_EU
```

Configuring Locations

You configure a location by using the **location** command in global server load-balancing configuration mode.

The syntax for this command is as follows:

```
location name [comments text | region name | zone name]
```

The keywords and arguments for this command are as follows:

- **name**—Geographical group name entities such as a city, data center, or content site for the location. Enter a unique alphanumeric name, with a maximum of 80 characters. Enter names that include spaces in quotes (for example, “name 1”).
- **comments**—(Optional) Specifies descriptive information or important notes about the location. Enter a maximum of 256 alphanumeric characters. Comments with spaces must be entered in quotes.
- **region name**—(Optional) Specifies a region with which the location will be associated. There should be a logical connection between the region and location. Enter a unique alphanumeric name, with a maximum of 80 characters. Enter names that include spaces in quotes (for example, “name 1”).

- **zone name**—(Optional) Specifies the name of an existing zone to be associated with the location. Specify this option if you are performing network proximity (see [Chapter 9, Configuring Network Proximity](#)). There should be a logical connection between the zone and the location.

For example, to create a location named San_Francisco and associate it with the region Western_USA, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# location SAN_FRANCISCO region
WESTERN_USA
gssm1.example.com(config-gslb)# location SAN_FRANCISCO comments "UNION
SQUARE"
```

If you need to delete a location, ensure that you know about the dependencies associated with a resource. For example, answers associated with locations that are deleted are automatically associated with the “Unspecified” location.



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

Before you delete a location to which an answer is associated, first change the location that is associated with the answer (see the “[Modifying an Answer](#)” section in [Chapter 6, Configuring Answers and Answer Groups](#)).

To delete a location use the **no location** command. For example, enter:

```
gssm1.example.com(config-gslb)# no location SAN_FRANCISCO
```

Configuring Owners

An owner is a logical grouping for GSS network resources that corresponds to a business or organizational structure. For example, an owner might be a hosting customer, an internal department such as human resources, or an IT staff resource.

As with locations, owner designations are used for the bulk management of GSS resources. Using a GSS owner to manage your answer group simplifies the process to suspend or activate all related answers.

You configure an owner by using the **owner** command in global server load-balancing configuration mode.

The syntax for this command is as follows:

```
owner name [comments text]
```

The keywords and arguments for this command are as follows:

- *name*—Logical name such as a business or organizational structure for the owner. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **comments** *text*—(Optional) Specifies descriptive information or important notes about the owner. Enter a maximum of 256 alphanumeric characters. Comments with spaces must be entered in quotes.

For example, enter:

```
gssm1.example.com# config  
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# owner WEB-SERVICES comments "INCLUDES  
MARKETING, ADVERTISING, AND ECOMMERCE CONTENT PROVIDERS"
```

If you need to delete an owner, be sure that you know the dependencies of that resource. For example, if you delete an owner, the answer groups, DNS rules, and domain lists associated with that owner will automatically be associated with the “System” owner account.



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

To delete an owner, enter:

```
gssm1.example.com(config-gslb)# no owner WEB-SERVICES comments
"INCLUDES MARKETING, ADVERTISING, AND ECOMMERCE CONTENT PROVIDERS"
```

Grouping GSS Resources by Location, Region, and Owner

After you create your locations, regions, and owners, group your GSS resources (an answer group, for example) by associating a resource with a location, region, or owner. Make this association at the command level of the CLI by specifying a grouping option and name. For example, when you enter the **domain list** command at the (config-gslb) prompt, specify the **owner** option followed by the name of an existing owner to associate the domain list with that owner. [Table 2-1](#) indicates which GSS resources can be grouped by locations, regions, and owners.

Table 2-1 GSS Network Groupings

GSS Network Resource	Grouped By
Locations	Region
Region	—
Owner	—
DNS rules	Owner
Source address lists	Owner
Domain lists	Owner
Answer group	Owner
Answer	Location

Displaying Resource Information

You use the **show gslb-config** command to display information about the resources currently configured for the GSS.

The keywords that display resource information for the **show gslb-config** command are as follows:

- **location**—Displays information about previously created locations.
- **owner**—Displays information about previously created owners.
- **region**—Displays information about previously created regions.

For example, to display a list of previously created regions, enter:

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

region Western_USA comments Denver, Portland, and Seattle
region Central_USA comments Chicago and Cleveland
region Eastern_USAcomments Boston, New York, and Atlanta
gssm1.example.com(config-gslb)#
```

Where to Go Next

[Chapter 3, Configuring Source Address Lists](#), describes the creation of source address lists. Source address lists are collections of IP addresses or address blocks for known client DNS proxies (or D-proxies).



Configuring Source Address Lists

This chapter describes how to configure DNS request handling on your GSS network by defining the IP addresses from which requests are sent to the GSS. Configure GSS request handling by creating source address lists and collections of IP addresses for known client DNS proxies (or D-proxies).

**Note**

The deployment of source address lists is an optional process. A default source address list, named Anywhere, is supplied with the GSS software and matches any request for a domain.

By using the source address lists feature, you can enter one or more IP addresses, with a maximum of 30 addresses for each list, to represent the DNS proxies from which requests originate. Each GSS supports a maximum of 60 source address lists.

This chapter contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Configuring Source Address Lists](#)
- [Displaying Source Address List Information](#)
- [Where to Go Next](#)

Logging in to the CLI and Enabling Privileged EXEC Mode



Note

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Configuring Source Address Lists

You configure a source address list by using the **source-address-list** command in global server load-balancing configuration mode.

The syntax for this command is as follows:

```
source-address-list name owner name [comments text]
```

The keywords and arguments for this command are as follows:

- **name**—Name for the source address list. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **owner name**—Specifies an existing owner name with which the source address list is to be associated. See the “Configuring Owners” section in [Chapter 2, Configuring Resources](#).
- **comments text**—(Optional) Specifies descriptive information or important notes about the source address list. Enter up to 256 alphanumeric characters. Comments with spaces must be entered in quotes.

After you enter the **source-address-list** command, the prompt changes to the source address list mode, where you specify IP addresses of the client DNS proxies. To enter multiple addresses, repeat the **ip address** command. You can enter a maximum of 60 addresses for each list, including the default list. With the default list, you cannot add any addresses because it is not user-configurable.

For example, to create a source address list named WEB-GLOBAL-LISTS and add two IP addresses and subnet masks to the list, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# source-address-list WEB-GLOBAL-LISTS
owner WEB-SERVICES comments "GLOBAL ALIST FOR ECOMMERCE"
gssm1.example.com(config-gslb-sal)# ip address 1024 172.27.16.4
255.255.255.0
gssm1.example.com(config-gslb-sal)# ip address 1024 172.27.28.4
255.255.255.0
```

If you need to delete a source address list, first verify that none of your DNS rules reference the source address list that you want to delete. You cannot delete source address lists associated with an existing DNS rule. If necessary, remove the source address list from the DNS rule. See [Chapter 7, Building and Modifying DNS Rules](#), for information about modifying a DNS rule.

**Caution**

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

To delete a source address list, perform the following steps:

1. If desired, use the **show gslb-config source-address-list** command to display information about the source address lists currently configured for the GSS. See the “[Displaying Source Address List Information](#)” section for more information.
2. Identify the source address list that you want to delete, and then use the **no** form of the **source-address-list** command to delete the address.

To display source address lists and delete a source address list, enter:

```
gssm1.example.com(config-gslb)# show gslb-config  
source-address-list  
  
source-address-list WEB-GLOBAL-LISTS owner WEB-SERVICES  
    ip address 192.168.1.0/24  
source-address-list sal2 owner WEB-SERVICES  
    ip address 192.168.100.0/24  
source-address-list Anywhere owner System  
    ip address 0.0.0.0/0  
  
gssm1.example.com(config-gslb)# no source-address-list  
WEB-GLOBAL-LISTS  
gssm1.example.com(config-gslb)#
```

To delete an IP address that is included in the source address list GLOBAL-SERVICE-LISTS, enter:

```
gssm1.example.com(config-gslb)# source-address-list  
GLOBAL-SERVICE-LISTS  
gssm1.example.com(config-gslb-sal)# no ip address 1024 172.27.16.4  
255.255.255.0  
gssm1.example.com(config-gslb-sal)#
```

Displaying Source Address List Information

You use the **show gslb-config source-address-list** command to display information about the source address lists currently configured for the GSS.

For example, to display previously created source address lists, enter:

```
gssm1.example.com(config-gslb)# show gslb-config source-address-list

source-address-list sal1 owner E-COMMERCE
    ip address 192.168.1.0/24
source-address-list sal2 owner WEB-SERVICES
    ip address 192.168.100.0/24
source-address-list sal3 owner SECURITY
    ip address 192.168.150.0/24
source-address-list Anywhere owner System
    ip address 0.0.0.0/0
gssm1.example.com(config-gslb)#
```

Where to Go Next

[Chapter 4, Configuring Domain Lists](#), describes the creation of domain lists. Domain lists are collections of domain names for Internet or intranet resources, sometimes referred to as hosted domains, that have been delegated to the GSS for DNS query responses.



Configuring Domain Lists

This chapter describes how to configure domain lists on your GSS network. Domain lists are collections of domain names for Internet or intranet resources, sometimes referred to as hosted domains, that have been delegated to the GSS for DNS query responses. Domain lists contain one or more domain names that point to content for which the GSS acts as the authoritative DNS server and for which you intend to use the GSS global server load-balancing technology to balance traffic and user requests.

Using domain lists, you can enter complete domain names or any valid regular expression that specifies a pattern by which the GSS can match incoming IP addresses.

Each GSS supports a maximum of 2000 hosted domains and 2000 hosted domain lists, with a maximum of 500 hosted domains supported for each domain list.

This chapter contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Configuring Domain Lists](#)
- [Displaying Domain List Information](#)
- [Where to Go Next](#)

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. Refer to the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the 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 the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Configuring Domain Lists

You configure a domain list using the **domain-list** command in global server load-balancing configuration mode.

The syntax for this command is as follows:

```
domain-list name [comments text | owner name]
```

The keywords and arguments for this command are as follows:

- **name**—Name for the new domain. Enter a unique alphanumeric name with a maximum of 80 characters. Spaces are not allowed.
- **comments** *text*—(Optional) Specifies descriptive information or important notes about the domain list. Enter a maximum of 256 alphanumeric characters. Comments with spaces must be entered in quotes.
- **owner** *name*—(Optional) Specifies an existing owner name with which the domain list is to be associated. See the “[Configuring Owners](#)” section in [Chapter 2, Configuring Resources](#).

After you enter the **domain-list** command, the prompt changes to the domain list mode, where you specify domains to be added to the domain list. To enter multiple domains, repeat the **domain** command in domain list mode. You can enter a maximum of 500 domains for each list. You can enter complete domain names or any regular expression that specifies a pattern by which the GSS can match incoming addresses. Enter the domain names of resources for which the GSS acts as the authoritative DNS server.

For example, to create a domain list called E-COMMERCE and add the domain DATABASEEXAMPLE.COM to the list, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# domain-list E-COMMERCE owner
WEB-SERVICES
gssm1.example.com(config-gslb)# domain-list E-COMMERCE comments
"GLOBAL DOMAIN LIST FOR ECOMMERCE"
gssm1.example.com(config-gslb-dl[dl-name])# domain DATABASEEXAMPLE.COM
```

Follow these guidelines when entering hosted domains:

- Domain names cannot exceed 128 characters. The following examples illustrate domain names configured on the GSS:

```
cisco.com
www.cisco.com
www.support.cisco.com
```

- If entering multiple domain names, repeat the **domain** command:

```
gssm1.example.com(config-gslb-dl[dl-name])# domain WWW.EXAMPLE.COM
gssm1.example.com(config-gslb-dl[dl-name])# domain
SUPPORT.EXAMPLE.COM
gssm1.example.com(config-gslb-dl[dl-name])# domain CDM.EXAMPLE.COM
```

- With the exception of the “?” wildcard, which is not supported, the GSS supports domain names that use wildcards. Wildcard syntax is based on POSIX 1003.2 extended regular expressions. Any request for a hosted domain that matches the pattern is directed accordingly.

For example, if you have 20 or more possible domains that the GSS is responsible for, such as `www1.cisco.com`, `www2.cisco.com`, and so on, you can create a wildcard expression that covers all of those domains. For example, enter:

```
.*\.cisco\.com
```

For domain names with wildcards that are valid regular expressions, the GSS can match strings up to 256 characters.



Note The use of the “?” wildcard is allowed for domain names only when using the **script play-config** command to play a GSLB configuration file. Refer to the “[File Modification Guidelines](#)” section in [Chapter 11, Creating and Playing GSLB Configuration Files](#), for more information.

If you need to delete a domain list, first verify that none of your DNS rules reference the domain list that you are about to delete. You cannot delete domain lists associated with an existing DNS rule. If necessary, remove the domain list from the DNS rule. Refer to [Chapter 7, Building and Modifying DNS Rules](#), for information about modifying a DNS rule.

**Caution**

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. Refer to the *Global Site Selector Administration Guide* for details.

To delete a domain list, enter:

```
gssm1.example.com(config-gslb)# no domain-list E-COMMERCE
```

To delete a domain from a domain list, enter:

```
gssm1.example.com(config-gslb-dl[dl-name])# no domain CDM.EXAMPLE.COM
```

Displaying Domain List Information

You use the **show gslb-config domain-list** command to display information about the domain lists currently configured for the GSS.

For example, to display previously created domain lists, enter:

```
gssm1.example.com(config-gslb)# show gslb-config domain-list
```

```
domain-list dl4 owner E-COMMERCE
  domain DATABASEEXAMPLE.COM
  domain EXAMPLE.COM
domain-list dl3 owner WEB-GLOBAL
  domain DATABASEEXAMPLE.COM
  domain EXAMPLE.COM
domain-list dl2 owner WEB-SERVICES
  domain DATABASEEXAMPLE.COM
domain-list dl1 owner System
  domain DATABASEEXAMPLE.COM
  domain EXAMPLE.COM
```

Where to Go Next

[Chapter 5, Configuring Keepalives](#), describes how to modify global keepalives and create shared keepalives.



Configuring Keepalives

This chapter describes how to configure keepalives on your GSS network. A keepalive is a method by which the GSS periodically checks to see if a resource associated with an answer is still active.

The GSS uses keepalives to collect and track information from the simple online status of VIPs to services and applications running on a server. You can configure a keepalive to continually monitor the online status of a resource and report that information to the primary GSSM.

Depending on the type of answer being tracked, the GSS also monitors load and connection information on server load balancers (SLBs) and then uses this information to perform load-based redirection.

This chapter contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Modifying Global Keepalive Properties](#)
- [Displaying Global Keepalive Properties](#)
- [Configuring Shared VIP Keepalives](#)
- [Configuring Scripted Keepalive Shared Keepalives](#)
- [Deleting a Shared Keepalive](#)
- [Displaying Shared Keepalive Properties](#)
- [Where to Go Next](#)

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Modifying Global Keepalive Properties

The GSS includes a set of global keepalive properties that function as the default (or minimum) values used by the GSS. If desired, you can modify the global keepalive properties for the GSS by entering CLI commands in the global server load-balancing configuration mode. Changing a global keepalive property and applying that change immediately modifies the default values of the keepalives currently in use by the GSS. For example, if a VIP answer uses a TCP keepalive with all of its associated defaults and you change the default port value from port 80 to port 23, port 23 automatically becomes the default for the TCP keepalive.

**Note**

You can also modify keepalive properties associated with an answer by changing keepalive properties in the answer configuration mode. See the “[Configuring and Modifying Answers](#)” section in [Chapter 6, Configuring Answers and Answer Groups](#) for more information.

To modify keepalive properties, use the **keepalive-properties** command in global server load-balancing configuration mode. The syntax for this command is as follows:

```
keepalive-properties { cra | http-head | icmp | kalap | scripted-kal | ns | tcp }
```

Specify the appropriate keepalive option type (**cra**, **http-head**, **icmp**, **kalap**, **scripted-kal**, **ns**, and **tcp**) to modify keepalive settings. This section provides detailed information about modifying and displaying global keepalive settings and contains the following topics:

- [Default Global Keepalive Properties and Settings](#)
- [Modifying ICMP Global Keepalive Settings](#)
- [Modifying TCP Global Keepalive Settings](#)
- [Modifying HTTP HEAD Global Keepalive Settings](#)
- [Modifying KAL-AP Global Keepalive Settings](#)
- [Modifying Scripted Keepalive Global Keepalive Settings](#)
- [Modifying CRA Global Keepalive Settings](#)
- [Modifying Name Server Global Keepalive Settings](#)

Default Global Keepalive Properties and Settings

Table 5-1 lists the GSS keepalive properties for all keepalive types and provides their default global settings. Where applicable, both Standard and Fast failure detection mode default settings are provided. The default Standard settings provide a keepalive failure detection time of 60 seconds. The default Fast settings provide a keepalive failure detection time of 4 seconds.

Table 5-1 *Default Global Keepalive Properties and Settings*

ICMP Global Keepalive Properties—Standard Failure Detection Mode	
Property	Default Global Setting
min-interval	40 seconds
ICMP Global Keepalive Properties—Fast Failure Detection Mode	
Property	Default Global Setting
retries	1
successful probes	1
TCP Global Keepalive Properties—Standard Failure Detection Mode	
Property	Default Global Setting
port	80
termination	reset
timeout	20 seconds
min-interval	40 seconds
TCP Global Keepalive Properties—Fast Failure Detection Mode	
Property	Default Global Setting
port	80
termination	reset
retries	1
successful probes	1

HTTP HEAD Global Keepalive Properties—Standard Failure Detection Mode

Property	Default Global Setting
port	80
path	/
termination	reset
timeout	20 seconds
min-interval	40 seconds

HTTP HEAD Global Keepalive Properties—Fast Failure Detection Mode

Property	Default Global Setting
port	80
path	"/"
termination	reset
retries	1
successful probes	1

KAL-AP Global Keepalive Properties—Standard Failure Detection Mode

Property	Default Global Setting
capp-key	hash-not-set
min-interval	40 seconds

KAL-AP Global Keepalive Properties—Fast Failure Detection Mode

Property	Default Global Setting
capp-key	hash-not-set
retries	1
successful probes	1

Scripted Keepalive Global Keepalive Properties—Standard Failure Detection Mode

Property	Default Global Setting
min-interval	40 seconds

Scripted Keepalive Global Keepalive Properties—Fast Failure Detection Mode

Property	Default Global Setting
retries	1

successful probes	1
CRA Global Keepalive Properties	
Property	Default Global Setting
cra-timing-decay	2
min-interval	10 seconds
Name Server Global Keepalive Properties	
Property	Default Global Setting
query-domain	“.”
min-interval	10 seconds

Modifying ICMP Global Keepalive Settings

To modify the ICMP global keepalive configuration settings, perform the following steps. See the [“Default Global Keepalive Properties and Settings”](#) section for a list of all default global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the [“Displaying Global Keepalive Properties”](#) section for more information.

You can modify an ICMP keepalive properties by changing either the Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.



Note The GSS supports a maximum of 750 ICMP keepalives when using the Standard detection method and a maximum of 150 ICMP keepalives when using the Fast detection method.

For more information on the keepalive detection time, see the [“Keepalives”](#) section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change the ICMP Standard settings by entering the **keepalive-properties icmp standard min-interval** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

keepalive-properties icmp standard min-interval *number*

The **min-interval *number*** keyword and argument specify the minimum frequency with which the GSS attempts to schedule ICMP keepalives. The valid entries are 40 to 255 seconds. The default is 40.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties icmp standard  
min-interval 60
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties icmp  
standard min-interval 60
```

3. Change the ICMP Fast settings by entering the **keepalive-properties icmp fast** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

keepalive-properties icmp fast {retries *number* | successful-probes *number*}

The keywords and arguments are as follows:

- **retries *number***—Specifies the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **successful-probes *number***—Specifies the number of consecutive successful ICMP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties icmp fast  
retries 3 successful-probes 2
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties icmp fast
retries 3 successful-probes 2
```

Modifying TCP Global Keepalive Settings

To modify the TCP global keepalive configuration settings, perform the following steps. See the “[Default Global Keepalive Properties and Settings](#)” section for a list of all default global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the “[Displaying Global Keepalive Properties](#)” section for more information.

You can modify TCP keepalive properties by changing either the Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.



Note The GSS supports a maximum of 1500 TCP keepalives when using the standard detection method and a maximum of 150 TCP keepalives when using the Fast detection method.

For more information on the keepalive detection time, see the “[Keepalives](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change the TCP Standard settings by entering the **keepalive-properties tcp standard** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties tcp standard {min-interval number} | port number |
termination {graceful | reset} | timeout number}
```

The keywords and arguments are as follows:

- **min-interval** *number*—Specifies the minimum frequency with which the GSS attempts to schedule TCP keepalives. The valid entries are 40 to 255 seconds. The default is 40.

- **port number**—Specifies the port on the remote device that is to receive the TCP-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.
- **termination**—Specifies one of the following TCP keepalive connection termination methods:
 - graceful**—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.
 - reset**—The GSS immediately terminates the TCP connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.
- **timeout number**—Specifies the length of time allowed before the GSS retransmits data to a device that is not responding to a request. The valid entries are 20 to 60 seconds. The default is 20.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# keepalive-properties tcp standard
min-interval 60 timeout 25
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties tcp
standard min-interval 60 timeout 25
```

3. Change the TCP Fast settings by entering the **keepalive-properties tcp fast** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties tcp fast {port number | retries number |
successful-probes number | termination {graceful | reset} }
```

The keywords and arguments are as follows:

- **port number**—Specifies the port on the remote device that is to receive the TCP-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.
- **retries number**—Specifies the number of times that the GSS retransmits a TCP packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect.

In those instances when the GSS is transmitting numerous TCP keepalives using port 23, be sure to change the value of the **retries** option. Valid entries range from 1 to 10, with a default of 1.



Note When using Graceful termination, two packets require acknowledgement: SYN and FIN.

- **successful-probes** *number*—Specifies the number of consecutive successful TCP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.
- **termination**—Specifies one of the following TCP keepalive connection termination methods:
 - graceful**—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.
 - reset**—The GSS immediately terminates the TCP connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# keepalive-properties tcp fast
retries 3 successful-probes 2 termination graceful
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties tcp fast
retries 3 successful-probes 2 termination graceful
```

Modifying HTTP HEAD Global Keepalive Settings

To modify the HTTP HEAD global keepalive configuration settings, perform the following steps. See the “[Default Global Keepalive Properties and Settings](#)” section for a list of all default global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the “[Displaying Global Keepalive Properties](#)” section for more information.

You can modify an HTTP HEAD keepalive properties by changing either the Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.

**Note**

The GSS supports a maximum of 500 HTTP HEAD keepalives when using the standard detection method and a maximum of 100 HTTP HEAD keepalives when using the fast detection method.

For more information on keepalive detection time, see the “[Keepalives](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change the HTTP HEAD Standard settings by entering the **keepalive-properties http-head standard** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties http-head standard { min-interval number } | path path | port number | termination { graceful | reset } | timeout number
```

The keywords and arguments are as follows:

- **min-interval** *number*—Specifies the minimum frequency with which the GSS attempts to schedule HTTP HEAD keepalives. The valid entries are 40 to 255 seconds. The default is 40.
- **path** *path*—Specifies the server website queried in the HTTP HEAD request (for example, /company/owner). The default path / specifies the virtual root of the webserver.

- **port number**—Specifies the port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.
- **termination**—Specifies one of the following HTTP HEAD keepalive connection termination methods:
 - graceful**—The GSS initiates the graceful closing of an HTTP HEAD connection by using the standard three-way connection termination method.
 - reset**—The GSS immediately terminates the TCP-formatted HTTP HEAD connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.
- **timeout number**—Specifies the length of time allowed before the GSS retransmits data to a device that is not responding to a request. The valid entries are 20 to 60 seconds. The default is 20.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# keepalive-properties http-head
standard min-interval 60 path /COMPANY/OWNER
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties http-head
standard min-interval 60 path /COMPANY/OWNER
```

3. Change the HTTP HEAD Fast settings by entering the **keepalive-properties http-head fast** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties http-head fast { path path | port number | retries
number | successful-probes number | termination { graceful | reset } }
```

The keywords and arguments are:

- **path path**—Specifies the server website queried in the HTTP HEAD request (for example, /company/owner). The default path “/” specifies the virtual root of the webserver.
- **port number**—Specifies the port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.

- **retries** *number*—Specifies the number of times that the GSS retransmits an HTTP HEAD packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.



Note When using graceful termination, three packets require acknowledgement: SYN, HEAD, and FIN.

- **successful-probes** *number*—Specifies the number of consecutive successful HTTP HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.
- **termination**—Specifies one of the following HTTP HEAD keepalive connection termination methods:
 - graceful**—The GSS initiates the graceful closing of an HTTP HEAD connection by using the standard three-way connection termination method.
 - reset**—The GSS immediately terminates the TCP-formatted HTTP HEAD connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties http-head  
fast path /COMPANY/OWNER retries 2 successful-probes 2
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties http-head  
fast path /COMPANY/OWNER retries 2 successful-probes 2
```

Modifying KAL-AP Global Keepalive Settings

To modify the KAL-AP global keepalive configuration settings, perform the following steps. See the [“Default Global Keepalive Properties and Settings”](#) section for a list of all global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the [Displaying Global Keepalive Properties](#) section for more information.

You can modify an KAL-AP keepalive properties by changing either the Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.



Note

The GSS supports a maximum of 128 primary and 128 secondary KAL-AP keepalives when using the standard detection method and a maximum of 40 primary and 40 secondary KAL-AP keepalives when using the fast detection method.

For more information on keepalive detection time, see the [“Keepalives”](#) section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change the KAL-AP Standard settings by entering the **keepalive-properties kalap standard** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties kalap standard { capp-key key | min-interval number }
```

The keywords and arguments are as follows:

- **capp-key** *key*—Specifies the secret key to be used for Content and Application Peering Protocol (CAPP) encryption. The alphanumeric string you enter is used to encrypt interbox communications using CAPP. You must also configure the same encryption value on the Cisco CSS or CSM.

- **min-interval** *number*—Specifies the minimum frequency with which the GSS attempts to schedule KAL-AP keepalives. The valid entries are 40 to 255 seconds. The default is 40.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties kalap  
standard capp-key SECRET-KEY-101 min-interval 80
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties kalap  
standard capp-key SECRET-KEY-101 min-interval 80
```

3. Change the KAL-AP Fast settings by entering the **keepalive-properties kalap fast** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties kalap fast {capp-key key | retries number |  
successful-probes number}
```

The keywords and arguments are as follows:

- **capp-key** *key*—Specifies the secret key to be used for Content and Application Peering Protocol (CAPP) encryption. The alphanumeric string you enter is used to encrypt interbox communications using CAPP. You must also configure the same encryption value on the Cisco CSS or CSM.
- **retries** *number*—Specifies the number of times that the GSS retransmits an KAL-AP packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **successful-probes** *number*—Specifies the number of consecutive successful KAL-AP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties kalap fast  
capp-key SECRET-KEY-101 retries 5 successful-probes 2
```

To reset the keepalive properties to the default settings, enter:

```
gssml.example.com(config-gslb)# no keepalive-properties kalap fast
capp-key SECRET-KEY-101 retries 5 successful-probes 2
```

Modifying ICMP Global Keepalive Settings

To modify the ICMP global keepalive configuration settings, perform the following steps. See “[Default Global Keepalive Properties and Settings](#)” for a list of all default global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the “[Displaying Global Keepalive Properties](#)” section for more information.

You can modify an ICMP keepalive properties by changing either the Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.



Note The GSS supports a maximum of 750 ICMP keepalives when using the standard detection method and a maximum of 150 ICMP keepalives when using the fast detection method.

For more information on keepalive detection time, see the “[Keepalives](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change the ICMP Standard settings by entering the **keepalive-properties icmp standard min-interval** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties icmp standard min-interval number
```

The **min-interval** *number* keyword and argument specify the minimum frequency with which the GSS attempts to schedule ICMP keepalives. The valid entries are 40 to 255 seconds. The default is 40.

For example, enter:

```
gssml.example.com(config)# gslb
```

```
gssm1.example.com(config-gslb)# keepalive-properties icmp standard  
min-interval 60
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties icmp  
standard min-interval 60
```

3. Change the ICMP Fast settings by entering the **keepalive-properties icmp fast** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties icmp fast {retries number | successful-probes  
number}
```

The keywords and arguments are as follows:

- **retries *number***—Specifies the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **successful-probes *number***—Specifies the number of consecutive successful ICMP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties icmp fast  
retries 3 successful-probes 2
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties icmp fast  
retries 3 successful-probes 2
```

Modifying Scripted Keepalive Global Keepalive Settings

To modify the Scripted keepalive global keepalive configuration settings, perform the following steps. See “[Default Global Keepalive Properties and Settings](#)” for a list of all default global keepalive settings.

1. Display the current property settings and failure detection mode for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the “[Displaying Global Keepalive Properties](#)” section for more information.

You can modify Scripted keepalive properties by changing either Standard or Fast failure detection mode properties. The requirements for your network should determine which failure detection mode (Fast or Standard) properties to modify.



Note

In the standard detection method, the GSS supports 256 Scripted keepalives if the Scripted keepalive is scalar and 128 if it is non-scalar. In the fast detection method, the GSS supports 60 Scripted keepalives if the Scripted keepalive is scalar and 30 if it is non-scalar.

For more information on keepalive detection time, see the “[Keepalives](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

2. Change Scripted keepalive Standard settings by entering the **keepalive-properties scripted-kal standard** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

keepalive-properties scripted-kal standard min-interval *number*

The keywords and arguments are as follows:

- **min-interval** *number*—Specifies the minimum frequency with which the GSS attempts to schedule Scripted keepalives. The valid entries are 40 to 255 seconds, with a default of 40.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# keepalive-properties scripted-kal
standard min-interval 60
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties  
scripted-kal standard min-interval 60
```

3. Change Scripted keepalive Fast settings by using the **keepalive-properties scripted-kal fast retries** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties scripted-kal fast retries number | successful-probes  
number
```

The keywords and arguments are as follows:

- **fast retries** *number*—Specifies the number of times that the GSS retransmits a Scripted keepalive packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries here are 1 to 5 attempts, with a default of 1.
- **successful-probes** *number*—Specifies the number of consecutive successful Scripted keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts, with a default of 1.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties scripted-kal  
fast retries 3 successful-probes 2
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties  
scripted-kal fast retries 3 successful-probes 2
```

Modifying CRA Global Keepalive Settings

To modify the CRA global keepalive configuration settings, perform the following steps. See the “[Default Global Keepalive Properties and Settings](#)” section for a list of all global keepalive settings.

1. Display the current property settings for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the “[Displaying Global Keepalive Properties](#)” section for more information.
2. Change the CRA settings by entering the **keepalive-properties cra** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties cra { min-interval number } | timing-decay number }
```

The keywords and arguments are as follows:

- **min-interval** *number*—Specifies the minimum frequency with which the GSS attempts to schedule CRA keepalives. The valid entries are 1 to 60 seconds. The default is 10.
- **timing-decay** *number*—Specifies how heavily the GSS should weigh recent DNS Round Trip Time (RTT) probe results relative to earlier RTT metrics. A setting of 1 indicates that recent results should not be weighed any more than previous RTT results. The valid entries are 1 to 10. The default is 2.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# keepalive-properties cra
min-interval 60 timing-decay 1
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties cra
min-interval 60 timing-decay 1
```

Modifying Name Server Global Keepalive Settings

To modify the Name Server (NS) global keepalive configuration settings, perform the following steps. See the [“Default Global Keepalive Properties and Settings”](#) section for a list of all global keepalive settings.

1. Display the current property settings for existing keepalives by entering the **show gslb-config keepalive-properties** command. See the [Displaying Global Keepalive Properties](#) section for more information.
2. Change the NS settings by entering the **keepalive-properties ns** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
keepalive-properties ns {min-interval number} | query-domain domain_name }
```

The keywords and arguments are as follows:

- **min-interval number**—Specifies the minimum frequency with which the GSS attempts to schedule NS keepalives. The valid entries are 40 to 255 seconds. The default is 40.
- **query-domain domain_name**—Specifies the name of the domain name server to which an NS-type keepalive is sent. Enter the name as an unquoted text string with no spaces and a maximum length of 100 characters. The default domain “.” specifies the root of the domain name server.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# keepalive-properties ns  
min-interval 60 query-domain WWW.HOME.COM
```

To reset the keepalive properties to the default settings, enter:

```
gssm1.example.com(config-gslb)# no keepalive-properties ns  
min-interval 60 query-domain WWW.HOME.COM
```

Displaying Global Keepalive Properties

You can use the **show gslb-config keepalive-properties** command to display the current property settings for all keepalives types.

The syntax of this command is as follows:

show gslb-config keepalive-properties

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# show gslb-config keepalive-properties

keepalive-properties scripted-kal standard min-interval 40
keepalive-properties icmp standard min-interval 40
keepalive-properties tcp fast retries 1 successful-probes 1
keepalive-properties http-head standard min-interval 40 port 80
termination reset timeout 20 path /
keepalive-properties kalap fast retries 1 successful-probes 1
keepalive-properties cra timing-decay 2 interval 10
keepalive-properties ns query-domain . interval 40
```

Configuring Shared VIP Keepalives

The GSS supports the use of shared keepalives to minimize traffic between the GSS and the SLBs that it is monitoring. A shared keepalive identifies a common IP address or resource that provides status for multiple answers. Shared keepalives periodically provide state information (online, offline) to the GSS for multiple VIP answer types. Once created, you can associate the shared keepalives with VIPs when you create a VIP answer type.



Note

Shared keepalives are not used with name server or CRA answers.

All answers are validated by configured keepalives and are not returned if the keepalive indicates that the answer is not viable. If a shared keepalive fails to return a status, the GSS assumes that all VIPs associated with that shared keepalive are offline.

If you intend to use the KAL-AP keepalive method with a VIP answer, you must configure a shared keepalive. The use of shared keepalives is an option for the ICMP, TCP, HTTP HEAD, and Scripted keepalive types.

This section contains the following topics:

- [Configuring ICMP Shared Keepalives](#)
- [Configuring TCP Shared Keepalives](#)

- [Configuring HTTP HEAD Shared Keepalives](#)
- [Configuring KAL-AP Shared Keepalives](#)
- [Configuring Scripted Keepalive Shared Keepalives](#)

Configuring ICMP Shared Keepalives

You can configure an ICMP shared keepalive by using the **shared-keepalive icmp** command in global server load-balancing configuration mode. Use the **no** form of the command to remove a shared keepalive. The syntax for this command is as follows:

```
shared-keepalive icmp ip_address
```

The *ip_address* argument specifies the IP address used to test the online status for the linked VIPs.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# shared-keepalive icmp 192.168.1.47  
gssm1.example.com(config-gslb)#
```

If you need to delete a shared keepalive from your GSS network, and that shared keepalive is in use by the GSS, you must first disassociate any answers that are using the keepalive. See the “[Configuring Scripted Keepalive Shared Keepalives](#)” section for more details.

Configuring TCP Shared Keepalives

You can configure a TCP shared keepalive by using the **shared-keepalive tcp** command in global server load-balancing configuration mode. Use the **no** form of the command to remove a shared keepalive.

The syntax for this command is as follows:

```
shared-keepalive tcp ip_address [port port_number] | [termination  
{graceful | reset}]
```

The keywords and arguments for this command are:

- *ip_address*—IP address used to test the online status for the linked VIPs.

- **port** *port_number*—(Optional) Specifies the port on the remote device that is to receive the TCP keepalive request. The port range is 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured setting.
- **termination**—(Optional) Specifies one of the following TCP keepalive connection termination methods. If you do not specify a connection termination method, the GSS uses the globally configured setting.
 - **graceful**—The GSS initiates the graceful closing of a HTTP HEAD connection by using the standard three-way connection termination method.
 - **reset**—The GSS immediately terminates the TCP connection by using a hard reset.

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# shared-keepalive tcp 192.168.1.46 port
23 termination graceful
```

Configuring HTTP HEAD Shared Keepalives

You can configure an HTTP HEAD shared keepalive by using the **shared-keepalive http-head** command in global server load-balancing configuration mode. Use the **no** form of the command to remove a shared keepalive.

The syntax for this command is as follows:

```
shared-keepalive http-head ip_address [port port_number] | [host-tag
domain_name] | [path path]
```

The keywords and arguments for this command are:

- *ip_address*—IP address used to test the online status for the linked VIPs.
- **port** *port_number*—(Optional) Specifies the port on the remote device that is to receive the HTTP HEAD-type keepalive request. The port range is 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured value.

- **host-tag** *domain_name*—(Optional) Specifies an optional domain name that is sent to the VIP as part of the HTTP HEAD query. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.
- **path** *path*—(Optional) Specifies the path that is relative to the server website being queried in the HTTP HEAD request. If you do not specify a default path, the GSS uses the globally configured value. The default path “/” specifies the virtual root of the webserver.

For example, enter:

```
gssml.example.com# config
gssml.example.com(config)# gslb
gssml.example.com(config-gslb)# shared-keepalive http-head
192.168.1.48 port 23 host-tag WWW.HOME.COM
```

Configuring KAL-AP Shared Keepalives

You can configure a KAL-AP shared keepalive by using the **shared-keepalive kalap** command in global server load-balancing configuration mode. Use the **no** form of the command to remove a shared keepalive.

The syntax for this command is as follows:

```
shared-keepalive kalap ip_address [secondary ip_address] | [capp-secure
enable [key secret]] | [retries number] | [successful-probes number]
```

The keywords and arguments for this command are:

- *ip_address*—IP address used to test the online status for the linked VIPs.
- **secondary** *ip_address*—(Optional) Specifies that the P address is to query a second Cisco CSS or CSM in a virtual IP (VIP) redundancy and virtual interface redundancy configuration.
- **capp-secure enable**—(Optional) Specifies that you wish to use Content and Application Peering Protocol (CAPP) encryption. If you do not specify an optional key (see below), the GSS uses the globally configured setting.
- **key** *secret*—(Optional) Specifies an encryption key that is used to encrypt interbox communications using CAPP. You must also configure the same encryption key on the Cisco CSS or CSM. Enter an unquoted alphanumeric text string with a maximum of 31 characters. If you do not specify a key, the GSS uses the globally configured setting.

If the KAL-AP global keepalive configuration is set to the Fast KAL Type, you can specify these parameters:

- **retries number**—(Optional) Specifies the number of times that the GSS retransmits a KAL-AP packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured setting.

For more information on keepalive detection time, see the [“Keepalives”](#) section in [Chapter 1, Introducing the Global Site Selector](#).

- **successful-probes number**—(Optional) Specifies the number of consecutive successful KAL-AP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it into the GSS network). The valid entries are 1 to 5. If you do not specify a value, the GSS uses the globally configured setting.

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# shared-keepalive kalap 192.168.1.40
secondary 192.168.1.42 retries
```

Configuring Scripted Keepalive Shared Keepalives

You can configure a Scripted keepalive shared keepalive by using the **shared-keepalive scripted-kal** command in global server load-balancing configuration mode. Use the **no** form of the command to remove a shared keepalive.

The syntax for this command is as follows:

```
shared-keepalive scripted-kal ip_address kal-name name
[ csm community community name | css community community name |
ios-slb community community name | snmp-mib-not-indexed-by-vip oid
oid community community name address-filter string load-filter string |
snmp-mib-indexed-by-vip oid oid community community name load-filter
string | snmp-scalar oid oid community community name ] [retries number]
| [successful-probes number]
```

The keywords and arguments for this command are:

- *ip_address*—IP address of the target device.
- **kal-name** *name*—Specifies the name of the applicable KAL. The answer attaches a Scripted keepalive to it.
- **csm community** *community name*—Configures the object identifiers (OIDs) and filter strings to select the load metric from a Catalyst 6500 series CSM's MIB.
- **css community** *community name*—Configures the OIDs and filter strings to select the load metric from a Cisco CSS's MIB.
- **ios-slb community** *community name*—Configures the OIDs and filter strings to select the load metric from a Cisco IOS MIB.

**Note**

To probe non-Cisco SLBs, you need to populate the OID, filter-string, and OID type.

- **snmp-mib-not-indexed-by-vip oid** *oid* **community** *community name* **address-filter** *string* **load-filter** *string*—Configures the OID, community, and filter strings to select the load metric from a remote machine. Two filters are required: a load filter and then an address filter.
- **snmp-mib-indexed-by-vip oid** *oid* **community** *community name* **load-filter** *string*—Configures the OID, community, and filter strings to select the load metric from a remote machine's MIB (indexed by a VIP address). The only required filter is the load filter.
- **snmp-scalar oid** *oid* **community** *community name*—Configures the OID and community to obtain a load from the target device.

[Table 5-2](#) lists the wrappers, OIDs, address, and load filters that are appropriate for different SLB devices.

**Note**

You are not required to use these OIDs and filter IDs. If you have the necessary information, you can use any other MIB. However, only the MIB and OIDs listed in [Table 5-2](#) have been tested and certified by Cisco Systems.

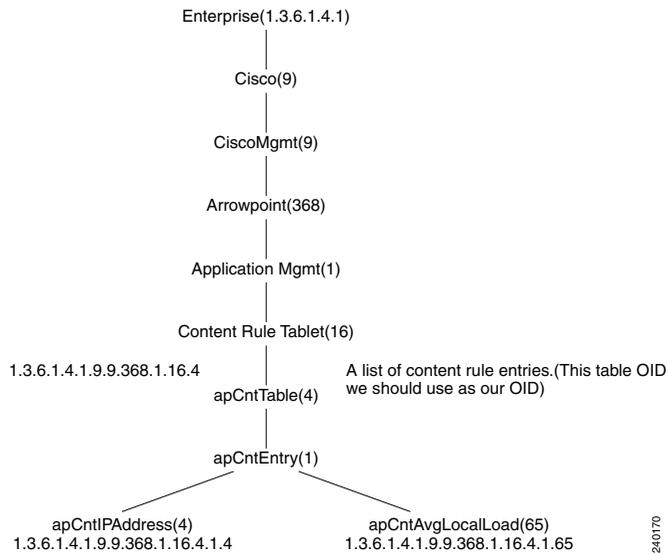
Table 5-2 MIBs, OIDs, and Filter IDs for Scripted Keepalive Types

Device	Scripted Keepalive Types	OID	Address Filter	Load Filter	Recommended Software Version
CSS	CSS wrapper	*	*	*	SLB: 7.40.0.04
	SNMP_mib_not_index_by_vip	1.3.6.1.4.1.9.9.368.1.16.4	1.4	1.65	
CSM	CSM wrapper	*	*	*	IOS: 12.2
	SNMP_mib_not_index_by_vip	1.3.6.1.4.1.9.9.161.1.4.1	1.4	1.17	CSM: 4.2(1)
IOS-SLB	IOS-SLB wrapper	*	*	*	IOS: 12.2
	SNMP_mib_not_index_by_vip	1.3.6.1.4.1.9.9.161.1.4.1	1.4	1.17	
F5	SNMP_mib_index_by_vip	1.3.6.1.4.1.3375.2.2.10.11.3	**N/A	1.11	SLB: 9.2.0 Build167.4

* Indicates that those fields are not user-configurable in that particular type of Scripted Keepalive. Those values are supplied internally by the software.

** Signifies that the address filter is not required in the case of SNMP_mib_index_by_vip.

You can also configure Scripted keepalives with any OID that represents load information on an SLB. Depending on the type of table, that is whether the load information is scalar, indexed by VIP, or not indexed by VIP, address and load filters may be required. [Figure 5-1](#) shows a configuration example using a CSS MIB tree.

Figure 5-1 CSS MIB Tree

In this tree, the OIDs are not indexed by VIP. One of the CSS tables that stores load information is `apCntTable` and the corresponding OID is `1.3.6.1.4.1.9.9.368.1.16.4`. From [Figure 5-1](#), you can see that the IP address of the pertinent VIP is referenced by the object `apCntIPAddress` (OID.1.4) and the load pertaining to this VIP is referenced by the object `apCntAvgLocalLoad` (OID.1.65). Thus, the IP address obtained here should populate the Address Filter, while the load information populates the Load Filter.

**Note**

If the load information in a MIB table is indexed by VIP, the only required filter is the load filter. Scalars will have neither address or load filters since there is no table associated with the OID.

If the Scripted keepalive global keepalive configuration is set to the Fast Scripted keepalive Type, you can specify these parameters:

- **retries number**—(Optional) Specifies the number of times that the GSS retransmits a Scripted keepalive packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time.

Reducing the number of retries has the reverse effect. The valid entries are 1 to 5 retries. If you do not specify a value, the GSS uses the globally configured setting.

For more information on the keepalive detection time, see the “Keepalives” section in [Chapter 1, Introducing the Global Site Selector](#).

- **successful-probes number**—(Optional) Specifies the number of consecutive successful Scripted keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it into the GSS network). The valid entries are 1 to 5. If you do not specify a value, the GSS uses the globally configured setting.

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# shared-keepalive scripted-kal
192.168.1.46 kal-name samplekal ios-slb community samplecommunity
```

Deleting a Shared Keepalive

To delete a shared keepalive that is in use by the GSS, you must first remove it from any answers that are using the keepalive.



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

To delete a shared keepalive, perform the following steps:

1. Display the current property settings for existing answers and keepalives by entering the **show gslb-config** command.
2. Identify the shared keepalive that you want to delete and the answer to which it is associated.
3. Enter the IP address and answer name (if the answer has a name) to access the answer vip configuration mode by using the **answer vip** command.
4. Remove the keepalive associated with the answer by entering the **no keepalive type** command in answer vip configuration mode.

5. Delete the shared keepalive by entering the **no shared-keepalive** command in global server load-balancing configuration mode.

For example, enter:

```
gssml.example.com(config-gslb)# show gslb-config
...
answer cra 192.168.50.41 delay 2 active
answer ns 172.16.27.4 DOMAIN EXAMPLE.COM active
answer vip 172.16.27.6 name ANSVIP2 active
    keepalive type tcp port 180 active
    keepalive type tcp port 88 active
...
gssml.example.com(config-gslb)# answer vip 172.16.27.6 name ANSVIP2
gssml.example.com(config-ansvip)# no keepalive type tcp port 88 active
gssml.example.com(config-ansvip)# exit
gssml.example.com(config-gslb)# no shared-keepalive tcp 172.16.27.6
gssml.example.com(config-gslb)#
```

Displaying Shared Keepalive Properties

You can use the **show gslb-config shared-keepalive** command to display information about the shared keepalives currently configured for the GSS.

For example, enter:

```
gssml.example.com(config-gslb)# show gslb-config shared-keepalive
...
shared-keepalive kalap 192.168.1.47 capp-secure enable
shared-keepalive tcp 192.168.1.46 termination graceful
shared-keepalive tcp 192.168.1.40
...
```

To display shared keepalive information for a specific IP address, enter:

```
gssml.example.com(config-gslb)# show gslb-config shared-keepalive
192.168.1.47
...
shared-keepalive kalap 192.168.1.47 capp-secure enable
...
```

Where to Go Next

[Chapter 6, Configuring Answers and Answer Groups](#), describes how to create and configure GSS answers and answer groups. Answers refer to resources to which the GSS resolves DNS requests that it receives. Once created, answers are grouped together as resource pools called answer groups.



Configuring Answers and Answer Groups

This chapter describes how to create and configure answers and answer groups for your GSS network. It contains the following major sections:

- [Configuring and Modifying Answers](#)
- [Configuring and Modifying Answer Groups](#)
- [Where to Go Next](#)

Configuring and Modifying Answers

In a GSS network, an answer refers to the resources that respond to content queries. When you create an answer using the primary GSSM, you are identifying a resource on your GSS network to which queries can be directed. This resource provides the requesting client D-proxy with the address of a valid host to serve the request.

GSS answers include the following:

- **VIP**—Virtual IP (VIP) addresses associated with an SLB such as the Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, Cisco LocalDirector, a web server, a cache, or any other geographically dispersed device in a global network deployment.
- **Name Server**—Configured DNS name server on your network that can answer queries that the GSS cannot resolve.

- CRA—Content routing agents that use a resolution process called DNS race to send identical and simultaneous responses back to a user's D-proxy.

The GSS groups answers together as resource pools, also referred to as answer groups. From the available answer groups, the GSS can use a maximum of three possible response answer group and balance method clauses in a DNS rule to select the most appropriate resource that serves a user request. Each balance method provides a different algorithm for selecting one answer from a configured answer group. Each clause specifies that a particular answer group serve the request and a specific balance method be used to select the best resource from that answer group.

Depending on the type of answer, the GSS can further analyze DNS queries to choose the best host. For example, a request that is routed to a VIP associated with a Cisco CSS is routed to the best resource based on load and availability, as determined by the CSS. A request that is routed to a CRA is routed to the best resource based on proximity, as determined in a DNS race conducted by the GSS.

This section contains the following topics:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Configuring a VIP-Type Answer](#)
- [Configuring a CRA-Type Answer](#)
- [Configuring a Name Server-Type Answer](#)
- [Modifying an Answer](#)
- [Displaying Answer Properties](#)
- [Suspending an Answer](#)
- [Reactivating an Answer](#)
- [Suspending or Reactivating All Answers in a Location](#)
- [Deleting an Answer](#)

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

Otherwise, if you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

2. Specify your GSS administrative username and password to log on to the GSSM. The CLI prompt appears.

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Configuring a VIP-Type Answer

When configuring a VIP-type answer, you can configure one of several different keepalive types or multiple keepalive types to test for that answer. See the [“Configuring Multiple Keepalives for a VIP Answer Type”](#) section for more information on configuring multiple keepalives to test for an answer. For a KAL-AP keepalive, configure shared keepalives before you configure your answer. See [Chapter 5, Configuring Keepalives](#) for more information on creating shared keepalives.

To configure a VIP-type answer, use the **answer vip** *ip_address* command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
answer vip ip_address [name name | location name | activate | suspend]
```

After you enter the **answer vip** *ip_address* command, the prompt changes to the answer vip configuration mode where you can optionally specify and configure keepalives for your VIP-type answer.

The keywords and arguments for this command are as follows:

- *ip_address*—VIP address field. Enter the VIP address to which the GSS will forward requests. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **name** *name*—(Optional) Specifies a name for the VIP-type answer that you are creating. Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **location** *name*—(Optional) Specifies an existing location name with which the answer is to be associated. See the “[Configuring Owners](#)” section in [Chapter 2, Configuring Resources](#).
- **activate**—(Optional) Reactivates a suspended VIP answer. This is the default setting.
- **suspend**—(Optional) Suspends an active VIP answer.

For example, to create a VIP answer called SEC-LONDON1 and associate it with the London location, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# answer vip 10.86.209.232 name
SEC-LONDON1 location LONDON
gssm1.example.com(config-ansvip[ans-ip])
```

To delete a VIP answer, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no answer vip 10.86.209.232 name
SEC-LONDON1 location LONDON
gssm1.example.com(config-gslb)
```

For more information on modifying existing answers, see the “[Modifying an Answer](#)” section.

This section contains the following topics:

- [Configuring Keepalive VIP Answers](#)
- [Configuring ICMP Keepalive VIP Answers](#)
- [Configuring TCP Keepalive VIP Answer Settings](#)
- [Configuring HTTP HEAD Keepalive VIP Answer Settings](#)
- [Configuring KAL-AP Keepalive VIP Answer Settings](#)
- [Configuring Scripted Keepalive VIP Answers](#)
- [Configuring Multiple Keepalives for a VIP Answer Type](#)

Configuring Keepalive VIP Answers

After you create an answer, you can choose to configure one of a variety of different keepalive types or multiple keepalive types to test for that answer.



Note

The default values used for each of the VIP keepalives are determined by the global keepalive property settings previously specified (see [Chapter 5, Configuring Keepalives](#)).

Configuring ICMP Keepalive VIP Answers

You can define the ICMP keepalives for your VIP answer by using the **keepalive type icmp** command in answer vip configuration mode. This command sends an ICMP echo message (ping) to the address specified for the VIP answer. The GSS determines the online status by the response received from the device, indicating simple connectivity to the network.

The syntax for this command is as follows:

```
keepalive type icmp [shared ip_address | retries number | successful-probes number]
```

The keywords and arguments for this command are as follows:

- **shared** *ip_address*—(Optional) Specifies the IP address of an existing ICMP shared keepalive. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1). See [Chapter 5, Configuring Keepalives](#), for more information on creating shared keepalives.

- **retries** *number*—(Optional) Specifies the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **successful-probes** *number*—(Optional) Specifies the number of consecutive successful ICMP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.

For example, to configure an ICMP keepalive for the VIP-type answer servicing VIP address 10.86.209.232, enter:

```
gssm1.example.com(config-gslb)# answer vip 10.86.209.232
gssm1.example.com(config-ansvip[ans-ip])# keepalive type icmp
retries 2
gssm1.example.com(config-ansvip[ans-ip])#
```

See the “[Configuring Multiple Keepalives for a VIP Answer Type](#)” section for details on configuring multiple keepalives to test for a VIP-type answer.

Configuring TCP Keepalive VIP Answer Settings

You can define the TCP keepalive for your VIP answer by using the **keepalive type tcp** command in answer vip configuration mode. This command sends a TCP handshake to the address specified for the VIP answer and port number of the remote device to determine service viability (three-way handshake and connection termination method), returning the online status of the device.

The syntax for this command is as follows:

```
keepalive type tcp [shared ip_address | port number | retries number |
successful-probes number | termination {graceful | reset}]
```

The keywords and arguments for this command are as follows:

- **shared** *ip_address*—(Optional) Specifies the IP address of an existing TCP shared keepalive. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1). See [Chapter 5, Configuring Keepalives](#) for more information on creating shared keepalives.

- **port number**—(Optional) Specifies the port on the remote device that is to receive the TCP-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.
- **retries number**—(Optional) Specifies the number of times the GSS retransmits a TCP packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **successful-probes number**—(Optional) Specifies the number of consecutive successful TCP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.
- **termination** —(Optional) Specifies one of the following TCP keepalive connection termination methods:
 - **graceful**—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.
 - **reset**—The GSS immediately terminates the TCP connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.

For example, to configure a TCP keepalive for the VIP-type answer servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1  
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 23  
successful-probes 4  
gssm1.example.com(config-ansvip[ans-ip])#
```

See the “[Configuring Multiple Keepalives for a VIP Answer Type](#)” section for details on configuring multiple keepalives to test for a VIP-type answer.

Configuring HTTP HEAD Keepalive VIP Answer Settings

You can define the HTTP HEAD keepalive for your VIP answer by using the **keepalive type http-head** command in answer vip configuration mode. This command sends a TCP-format HTTP HEAD request to an origin web server at the address specified for the VIP answer. The GSS determines the online status of the device in the form of an HTTP Response Status Code of 200 (for example, HTTP/1.0 200 OK) from the server as well as information on the web page status and content size.

The syntax for this command is as follows:

```
keepalive type http-head [host-tag domain_name | path path | port number
| retries number | shared ip_address | successful-probes number |
termination {graceful | reset}]
```

The keywords and arguments for this command are as follows:

- **host-tag** *domain_name*—(Optional) Specifies an optional domain name that is sent to the VIP as part of the HTTP HEAD query. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.
- **path** *path*—(Optional) Specifies the server website queried in the HTTP HEAD request (for example, /company/owner). The default path “/” specifies the virtual root of the webserver.
- **port** *number*—(Optional) Specifies the port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS. The valid entries are 1 to 65535. The default port is 80.
- **retries** *number*—(Optional) Specifies the number of times that the GSS retransmits an HTTP HEAD packet before declaring the device offline. As you adjust the retries value, you change the detection time determined by the GSS. By increasing the number of retries, you increase the detection time. Reducing the number of retries has the reverse effect. The valid entries are 1 to 10 retries. The default is 1.
- **shared** *ip_address*—(Optional) Specifies the IP address of an existing HTTP HEAD shared keepalive. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1). See [Chapter 5, Configuring Keepalives](#) for more information on creating shared keepalives.

- **successful-probes *number***—(Optional) Specifies the number of consecutive successful HTTP HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. The valid entries are 1 to 5 attempts. The default is 1.
- **termination**—(Optional) Specifies one of the following HTTP HEAD keepalive connection termination methods:
 - **graceful**—The GSS initiates the graceful closing of an HTTP HEAD connection by using the standard three-way connection termination method.
 - **reset**—The GSS immediately terminates the TCP-formatted HTTP HEAD connection by using a hard reset. If you do not specify a connection termination method, the GSS uses this method type.

For example, to configure an HTTP HEAD keepalive for the VIP-type answer servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1
gssm1.example.com(config-ansvip[ans-ip])# keepalive type http-head
host-tag WWW.HOME.COM termination graceful
gssm1.example.com(config-ansvip[ans-ip])#
```

See the “[Configuring Multiple Keepalives for a VIP Answer Type](#)” section for details on configuring multiple keepalives to test for a VIP-type answer.

Configuring KAL-AP Keepalive VIP Answer Settings

You can define the KAL-AP keepalive for your VIP answer by using the **keepalive type kalap** command in answer vip configuration mode. This command sends a detailed query to the Cisco CSS or CSM at the address specified for the VIP answer to extract the load and availability. The GSS determines the online status when the SLBs respond with information about a hosted domain name, host VIP address, or a configured tag on a content rule.

The syntax for this command is as follows:

```
keepalive type kalap {tag ip_address {tag_name} | vip ip_address}
```

The keywords and arguments for this command are as follows:

- **tag *ip_address***—Specifies the shared KAL-AP-type keepalive address in the KAL-AP request. The KAL-AP queries the keepalive address to determine the online status. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).

- *tag_name*— An alphanumeric tag associated with the VIP in the KAL-AP request. The tag value is used to match the correct shared keepalive VIP, thus avoiding the confusion that may be caused when probing for the status of a VIP located behind a firewall network address translation (NAT). Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- *vip ip_address*—Specifies the shared KAL-AP-type keepalive address in the KAL-AP request. The KAL-AP queries the keepalive address to determine the online status. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).

For example, to configure a KAL-AP keepalive for the VIP-type answer servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1
gssm1.example.com(config-ansvip[ans-ip])# keepalive type kalap tag
192.168.50.41 TAG1
gssm1.example.com(config-ansvip[ans-ip])#
```

See the “[Configuring Multiple Keepalives for a VIP Answer Type](#)” section for details on configuring multiple keepalives to test for a VIP-type answer.

The Content and Application Peering Protocol (CAPP) may not recognize dropped fragments when a KAL-AP keepalive spans multiple datagrams due to large payloads. When the KAL-AP keepalive spans multiple datagrams and one of the spanned packets is dropped, the GSS does not retry the request. Instead, the GSS waits until the next period and sends the packets again, which results in the dropped datagram not getting updated load values on the VIPs that expect them. This behavior occurs when the GSS consumes the full datagram (roughly 1.4 K) with tag names or VIP addresses. Otherwise, all data fits in a single datagram.

Use the VIP format for KAL-AP when you need the GSS to send a detailed query on load for hundreds of VIPs configured to a single primary or optional secondary (backup) IP address. You can also use the tag format for KAL-AP. However, you must limit the length of the tag name to ensure that the packets do not exceed 1.4K.

Configuring Scripted Keepalive VIP Answers

You can define the Scripted keepalives for your VIP answer by using the **keepalive type scripted-kal** command in answer vip configuration mode. This command allows you to specify a KAL name and maximum load in order to add a Scripted keepalive probe to the VIP.

The syntax for this command is as follows:

```
keepalive type scripted-kal kal-name name max-load max load value
```

The keywords and arguments for this command are as follows:

- **kal-name** *name*—Specifies the name of an existing Scripted keepalive shared keepalive. See [Chapter 5, Configuring Keepalives](#) for more information on creating shared keepalives.
- **max-load** *max load value*—Specifies the maximum allowable load when adding a Scripted keepalive probe to the VIP.

For example, to configure a Scripted keepalive for the VIP-type answer servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1  
gssm1.example.com(config-ansvip[ans-ip])# keepalive type scripted-kal  
kal-name samplekal max-load 50  
gssm1.example.com(config-ansvip[ans-ip])#
```

See the “[Configuring Multiple Keepalives for a VIP Answer Type](#)” section for details on configuring multiple keepalives to test for a VIP-type answer.

Configuring Multiple Keepalives for a VIP Answer Type

The primary GSSM allows you to assign multiple keepalives and/or destination ports for a single VIP answer. You can configure a maximum of five different keepalives for a VIP answer, in a mix and match configuration of ICMP, TCP, HTTP HEAD, and KAL-AP VIP keepalive types. However, the primary GSSM supports only a single usage of a shared keepalive and a single KAL-AP keepalive when you specify multiple keepalive types.

For TCP or HTTP HEAD keepalives, you may also specify different destination ports. The multi-port keepalive capability allows you to monitor a single server and check responses from multiple ports. If the keepalives are successful, the GSS device considers the resource active and continues to redirect client traffic to the

server. Servers that yield unsuccessful connections are marked as unavailable; subsequent successful connections to the server will reinstate it as available to be used as a resource.

When using multiple keepalive types, the VIP answer status is a logical AND function of all keepalive probes associated with an answer, resulting in a consolidation of results from each answer.

For example, to configure a group of five keepalives that include a mix of shared and nonshared TCP-, -ICMP, and HTTP HEAD-type keepalives servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 443
ip-address 192.168.50.41 retries 3 successful-probes 4 termination
reset
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 80
retries 4
gssm1.example.com(config-ansvip[ans-ip])# keepalive type http-head
port 8080 ip-address 10.86.209.22 termination graceful
gssm1.example.com(config-ansvip[ans-ip])# keepalive type icmp
ip-address 10.86.209.4 shared
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 1650
ip-address 10.86.209.4 shared
gssm1.example.com(config-ansvip[ans-ip])# exit
gssm1.example.com(config-gslb)#
```

To configure TCP- and HTTP HEAD-type keepalives for multiple ports for the VIP-type answer named MPORT_KALE_MIX that services VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1 name
MPORT_KALE_MIX
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 80
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 443
gssm1.example.com(config-ansvip[ans-ip])# keepalive type http-head
port 8080
gssm1.example.com(config-ansvip[ans-ip])# exit
gssm1.example.com(config-gslb)#
```



Note

When you configure multiple keepalives for an answer and you are using a KAL-AP-type keepalive, you can configure only one KAL-AP-type keepalive, which you must specify as the first keepalive.

To configure KAL-AP-, TCP- and HTTP HEAD-type keepalives for the VIP-type answer servicing VIP address 192.168.200.1, enter:

```
gssm1.example.com(config-gslb)# answer vip 192.168.200.1
gssm1.example.com(config-ansvip[ans-ip])# keepalive type kalap tag
192.168.50.41 TAG1
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 80
gssm1.example.com(config-ansvip[ans-ip])# keepalive type tcp port 443
gssm1.example.com(config-ansvip[ans-ip])# keepalive type http-head
port 8080
gssm1.example.com(config-ansvip[ans-ip])# exit
gssm1.example.com(config-gslb)#
```

Configuring a CRA-Type Answer

The content routing agent (CRA) answer type relies on content routing agents and the GSS to choose a suitable answer for a given query based on the proximity of two or more possible hosts to the requesting D-proxy.

With the CRA-type answer, the requests received from a particular D-proxy are served by the content server that responds first to the request. The response time is measured using a DNS race and is coordinated by the GSS and content routing agents running on each content server. In the race, multiple hosts respond simultaneously to a request. The server with the fastest response time (the shortest network delay between itself and the client's D-proxy) is chosen to serve the content.

The CRA-type answer is designed to work with the GSS when you select the boomerang balance method with a DNS rule (utilizing the boomerang server component of the GSS).

Closeness is determined when multiple hosts reply to the requesting D-proxy simultaneously in what is referred to as a “DNS race.” The GSS coordinates the start of the race so that all CRAs initiate their response at the same time. The first DNS reply to reach the D-proxy is chosen by the name server as the host containing the answer.

To configure a CRA-type answer, use the **answer cra ip_address** command in global server load-balancing configuration mode. The syntax of this command is as follows:

```
answer cra ip_address [enable | disable | delay number | name name |  
location name | activate | suspend]
```

The keywords and arguments for this command are as follows:

- *ip_address*—Interface or circuit address of the CRA. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **enable**—(Optional) Specifies that the GSS is to perform keepalive checks on the answer. This is the default setting. Use the **disable** keyword if you plan to specify a one-way delay to calculate a static RTT. See the **delay** keyword for information on static RTT.
- **disable**—(Optional) Specifies that the GSS use the one-way **delay** keyword to calculate a static round-trip time (RTT). See the **delay** keyword for more information on static RTT.
- **delay number**—(Optional) Specifies a one-way delay time in milliseconds. This value is used by the GSS to calculate a static round-trip time (RTT), with the one-way delay constituting one-half of the round-trip time that is used for all DNS races involving this answer. Valid entries are 0 to 1000 milliseconds. The default is 0.
- **name name**—(Optional) Specifies a name for the CRA-type answer. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **location name**—(Optional) Specifies an existing location name with which the answer is to be associated. See the “[Configuring Owners](#)” section in [Chapter 2, Configuring Resources](#).
- **activate**—(Optional) Reactivates a suspended CRA answer. This is the default.
- **suspend**—(Optional) Suspends an active CRA answer.

For example, to create a CRA-type answer with a one-way delay, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# answer cra 10.86.209.22 name CRA-ANS1
delay 3
gssm1.example.com(config-gslb)
```

To delete a CRA-type answer, enter:

```
gssm1.example.com(config-gslb)# no answer cra 10.86.209.22 name
CRA-ANS1 delay 3
gssm1.example.com(config-gslb)
```

For information on modifying existing answers, see the [“Modifying an Answer”](#) section.

Configuring a Name Server-Type Answer

A name server (NS)-type answer specifies the IP address of a DNS name server to which DNS queries are forwarded from the GSS. Using the name server forwarding feature, queries are forwarded to a non-GSS name server for resolution, with the answer passed back to the GSS name server and from there to the requesting D-proxy. The name server-type answer acts as a guaranteed fallback resource. A fallback resource can resolve requests that the GSS cannot resolve itself either because the requested content is unknown to the GSS or because the resources that typically handle such requests are unavailable.

To configure a NS-type answer, use the **answer ns *ip_address*** command in global server load-balancing configuration mode. The syntax of this command is:

```
answer ns ip_address [enable | disable | name name | domain name | location name | activate | suspend]
```

The keywords and arguments for this command are as follows:

- *ip_address*—Name server that the GSS uses to forward its requests. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **enable**—(Optional) Specifies that the GSS is to perform keepalive checks on the specified name server. The GSS queries the name server IP address to determine online status. This is the default.
- **disable**—(Optional) Specifies that the GSS disable keepalive checks on the specified name server. The GSS assumes that the name server is always online.
- **name *name***—(Optional) Specifies a name for the NS-type answer. Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **domain *name***—(Optional) Specifies the name of the domain name server to which an NS-type keepalive is sent (to determine the online status). Enter the name as an unquoted text string with no spaces and a maximum length of 100 characters (for example, www.home.com).



Note If no domain is specified, the GSS queries the globally configured query domain. For instructions on configuring the global query domain, see [Chapter 5, Configuring Keepalives](#).

- **location name**—(Optional) Specifies an existing location name with which the answer is to be associated. See the “[Configuring Owners](#)” section in [Chapter 2, Configuring Resources](#).
- **activate**—(Optional) Reactivates a suspended NS answer. This is the default.
- **suspend**—(Optional) Suspends an active NS answer.

For example, to create an NS-type answer that specifies a domain name server, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# answer ns 10.86.209.4 domain
WWW.HOME.COM enable
gssm1.example.com(config-gslb)
```

To delete a NS-type answer, enter:

```
gssm1.example.com(config-gslb)# no answer ns 10.86.209.4 domain
WWW.HOME.COM enable
gssm1.example.com(config-gslb)
```

For information on modifying existing answers, see the “[Modifying an Answer](#)” section.

Modifying an Answer

Once you have configured your answers, you can modify them at any time. However, once an answer is created and named, you cannot modify its type (for example, from VIP to CRA), its IP address, or its name.

To modify an existing answer, perform the following steps:

1. Display the current property settings for answers by entering the **show gslb-config answer** command. See the “[Displaying Answer Properties](#)” section for more information.
2. Change settings for an answer by entering the **answer** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
answer { cra | ns | vip }
```

The options are as follows:

- **cra**—Specifies a CRA-type answer for modification. See the “[Configuring a CRA-Type Answer](#)” section for details on how to modify CRA-type properties.
- **ns**—Specifies an NS-type answer for modification. See the “[Configuring a Name Server-Type Answer](#)” section for details on how to modify NS-type properties.
- **vip**—Specifies a VIP-type answer for modification. See the “[Configuring a VIP-Type Answer](#)” section for details on how to modify VIP-type properties. Also, See the “[Configuring Keepalive VIP Answers](#)” section for information on modifying keepalives for VIP-type answers.

For example, to first display the answer property settings, and then change the one-way delay time for an existing CRA-type answer, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer
...
answer cra 192.168.50.41 delay 2 activate
answer ns 172.16.27.4 domain EXAMPLE.COM activate
answer vip 172.16.27.6 name ansvip2 activate
    keepalive type tcp port 180 activate
    keepalive type tcp port 88 activate
...
gssm1.example.com(config-gslb)# answer cra 192.168.50.41 delay 5
gssm1.example.com(config-gslb)#
```

In order to modify a named answer, you must specify its name, type, and IP address. For example, to modify the answer named ANSVIP2, enter:

```
gssm1.example.com(config-gslb)# answer vip 172.16.27.6 name
ANSVIP2 delay 100
gssm1.example.com(config-gslb)#
```

Displaying Answer Properties

You can use the **show gslb-config answer** command to display the current property settings for all answer types.

The syntax of this command is as follows:

```
show gslb-config answer
```

For example, enter:

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

answer cra 192.168.50.41 delay 2 active
answer ns 172.16.27.4 domain EXAMPLE.COM active
answer vip 172.16.27.6 name ansvip2 active
    keepalive type tcp port 180 active

answer vip 192.168.50.30 active
    keepalive type tcp port 88 active

answer vip 192.168.50.2 name ansvip active
    keepalive type icmp active
    keepalive type tcp port 88 active
    keepalive type tcp port 80 active
gssm1.example.com(config-gslb)#
```

To display the property settings based on the IP address and answer type, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer 172.16.27.6
vip

answer vip 172.16.27.6 name ansvip2 active
    keepalive type tcp port 180 active
gssm1.example.com(config-gslb)#
```

To display the property settings based on an answer name, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer ansvip2

answer vip 172.16.27.6 name ansvip2 active
    keepalive type tcp port 180 active
gssm1.example.com(config-gslb)#
```

Suspending an Answer

You can temporarily stop the GSS from using an active answer by modifying the answer with the **suspend** keyword in the **answer** command. Suspending prevents that answer from being used by any of the currently configured DNS rules.

**Note**

You can suspend multiple answers associated with an answer group by using the **no activate-all-answers** command. See the [“Suspending or Reactivating All Answers in an Answer Group”](#) section for details.

To suspend an answer, perform the following steps:

1. Display the current answers by entering the **show gslb-config answer** command. See the [“Displaying Answer Properties”](#) section for more information.
2. Identify the active answer that you want to suspend, and then use the **answer** command with the **suspend** keyword to suspend the answer.

For example, to suspend the NS-type answer that queries the domain server at EXAMPLE.COM, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer
...
answer cra 192.168.50.41 delay 2 active
answer ns 172.16.27.4 domain EXAMPLE.COM active
answer vip 172.16.27.6 name ansvip2 active
      keepalive type tcp port 180 active
...
gssm1.example.com(config-gslb)# answer ns 172.16.27.4 domain
EXAMPLE.COM suspend
gssm1.example.com(config-gslb)#
```

To reactivate a suspended answer, use the activate feature (see the [“Reactivating an Answer”](#) section).

Reactivating an Answer

You can reactivate a suspended answer by modifying the specific answer with the **activate** keyword (for the **answer** command).

To reactivate an answer, perform the following steps:

1. Display the current answers by entering the **show gslb-config answer** command. See the “[Displaying Answer Properties](#)” section for more information.
2. Identify the active answer that you want to reactivate, and then use the **answer** command with the **activate** keyword to reactivate the answer.

For example, to reactivate the NS-type answer that queries the domain server at EXAMPLE.COM, enter:

```
gssml.example.com(config-gslb)# show gslb-config answer
...
answer cra 192.168.50.41 delay 2 active
answer ns 172.16.27.4 domain EXAMPLE.COM suspend
answer vip 172.16.27.6 name ansvip2 active
    keepalive type tcp port 180 active
...
gssml.example.com(config-gslb)# answer ns 172.16.27.4 domain
EXAMPLE.COM activate
gssml.example.com(config-gslb)#
```

Suspending or Reactivating All Answers in a Location

You can group and manage answers according to an established GSS location. Using a location to manage your answers makes it easier for you to quickly suspend or activate answers in a particular area of your network, for example, shutting down one or more data centers to perform software upgrades or regular maintenance.

The GSS automatically detects and routes requests around suspended answers.



Note

Suspending all answers in a location overrides the active or suspended state of an individual answer.

To suspend or reactivate answers based on their location, use the **location** command with the **suspend-all-answers** and **activate-all-answers** options.

Use the **show gslb-config location** command to display the currently configured locations. See [Chapter 2, Displaying Resource Information](#), for more information about this command.

For example, to suspend all answers based on the location Normandy, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# location Normandy suspend-all-answers
gssm1.example.com(config-gslb)#
```

To reactivate all answers based on the location Normandy, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# location Normandy activate-all-answers
gssm1.example.com(config-gslb)#
```

Deleting an Answer



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

To delete an answer, perform the following steps:

1. Display the current answers by entering the **show gslb-config answer** command. See the “[Displaying Answer Properties](#)” section for more information.
2. Identify the active answer that you want to delete, and then use the **no** form of the **answer** command to delete the answer.

For example, to delete the VIP-type answer that queries IP address 192.168.50.30 and all keepalives for that answer, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer
...
answer cra 192.168.50.41 delay 2 activate
answer ns 172.16.27.4 domain EXAMPLE.COM activate
answer vip 172.16.27.6 name ansvip2 activate
    keepalive type tcp port 180 activate

answer vip 192.168.50.30 activate
    keepalive type tcp port 88 activate

answer vip 192.168.50.2 name ansvip activate
    keepalive type icmp activate
    keepalive type tcp port 88 activate
    keepalive type tcp port 80 activate
```

```

keepalive type tcp activate
...
gssm1.example.com(config-gslb)# no answer vip 192.168.50.30
gssm1.example.com(config-gslb)#

```

In order to delete a named answer, you must specify its name, type, and IP address. For example, to delete the answer named ANSVIP2, you must enter:

```

gssm1.example.com(config-gslb)# no answer vip 172.16.27.6 name
ANSVIP2
gssm1.example.com(config-gslb)#

```

Configuring and Modifying Answer Groups

Answer groups are lists of GSS resources that are candidates to respond to DNS queries received from a user for a hosted domain. By using the DNS rules feature, you associate these lists of network resources with one of the following balance methods used to resolve the request:

- For a VIP answer group type, the GSS selects one or more VIPs using the balance method specified in the DNS rule.
- For a CRA answer group type, all CRAs in the answer group are queried and then race to respond first to the D-proxy with their IP address.
- For a name server answer group type, the GSS selects a name server using the balance method specified in the DNS rule and forwards the client's request to that name server.

A DNS rule can have a maximum of three balance clauses. Each balance clause specifies a different answer group from which an answer can be chosen after taking load threshold, order, and weight factors into account for each answer.

Before creating your answer groups, configure the answers that make up those groups. See the “[Configuring and Modifying Answers](#)” section for more information on creating GSS answers.

This section contains the following topics:

- [Creating an Answer Group](#)
- [Modifying an Answer Group](#)
- [Adding or Deleting an Authority Domain in an Answer Group](#)
- [Suspending or Reactivating All Answers in an Answer Group](#)

- [Suspending or Reactivating All Answers in Answer Groups Associated with an Owner](#)
- [Displaying Answer Group Properties](#)
- [Deleting an Answer Group](#)

Creating an Answer Group

You can configure up to 1000 answer groups on the primary GSSM. To create an answer group, use the **answer-group** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
answer-group name {owner name type {cra | ns | vip}}
```

After you enter the **answer-group** command, the prompt changes to the answer group configuration mode, where you add previously configured answers to the group.

The keywords and arguments for this command are as follows:

- *name*—Name for the answer group. Enter a unique alphanumeric name with a maximum of 80 characters. Names should not contain spaces.
- **owner** *name*—Specifies the name of an existing owner with which the answer group will be associated. For details about creating an owner, see [Chapter 2, Configuring Resources](#).
- **type**—Specifies a type for the answer group. The following options are available:
 - **cra**—The answer group consists of content routing agents (CRAs) for use with the boomerang server component of the GSS.
 - **ns**—The answer group consists of configured name servers.
 - **vip**—The answer group consists of virtual IPs controlled by an SLB device such as a CSS or CSM.

For example, to create a VIP answer group, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP1 owner  
WEB-SERVICES type vip  
gssm1.example.com(config-gslb-agvip[ag-name])#
```

For example, to delete a VIP answer group, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no answer-group ANSGRPVIP1 owner
WEB-SERVICES type vip
gssm1.example.com(config-gslb)#
```

This section contains the following topics:

- [Adding Answers to a CRA-Type Answer Group](#)
- [Adding Answers to an NS-Type Answer Group](#)
- [Adding Answers to a VIP-Type Answer Group](#)

Adding Answers to a CRA-Type Answer Group

After you create a CRA-type answer group, add previously configured CRA-type answers to the group using the **answer-add** command in the answer group configuration mode.

The syntax for this command is as follows:

```
answer-add ip_address [activate | name | suspend]
```

The keywords and arguments for this command are as follows:

- *ip_address*—IP address of a previously configured CRA-type answer. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **activate**—(Optional) Reactivates a suspended CRA answer. This is the default.
- **name**—(Optional) Specifies the name of a previously configured CRA-type answer. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **suspend**—(Optional) Suspends an active CRA answer.

For example, to add answers to and configure a CRA answer group, enter:

```
gssm1.example.com(config-gslb-agcra[ag-name])# answer-add 192.168.10.1
name www-boston-1
gssm1.example.com(config-gslb-agcra[ag-name])# answer-add 192.172.24.1
name www-ny-1
gssm1.example.com(config-gslb-agcra[ag-name])# answer-add 192.186.14.1
name www-atlanta-1
gssm1.example.com(config-gslb-agcra[ag-name])#
```

To delete an answer from a CRA answer group, enter:

```
gssm1.example.com(config-gslb-agcra[ag-name])# no answer-add
192.186.14.1 name www-atlanta-1
```

Adding Answers to an NS-Type Answer Group

After you create an NS-type answer group, add previously configured NS-type answers to the group using the **answer-add** command in the answer group configuration mode.

The syntax for this command is as follows:

```
answer-add ip_address [name | order number | weight number | activate | suspend]
```

The keywords and arguments for this command are as follows:

- *ip_address*—IP address of a previously configured NS-type answer. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **name**—(Optional) Specifies the name of a previously configured NS-type answer. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **order number**—(Optional) Assigns the specified order to the answer that is to be added to the answer group. Specify this option when using an ordered balance method type. Valid entries are 0 to 65535.
- **weight number**—(Optional) Assigns the specified weight to the answer that is to be added to the answer group. Specify this option when using a weighted round-robin or least-loaded balance method type. Valid entries are 1 to 10.

For more information on the order and weight settings, see the “[Balance Methods](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

- **activate**—(Optional) Reactivates a suspended NS answer. This is the default.
- **suspend**—(Optional) Suspends an active NS answer.

For example, to add answers to and configure an NS answer group, enter:

```
gssm1.example.com(config-gslb-agns[ag-name])# answer-add 192.168.10.1
name www-zurich-1 order 10
gssm1.example.com(config-gslb-agns[ag-name])# answer-add 192.172.20.1
name www-barcelona-1 order 20
gssm1.example.com(config-gslb-agns[ag-name])# answer-add 192.188.30.1
name www-brussels-30
gssm1.example.com(config-gslb-agns[ag-name])#
```

To delete an answer from an NS answer group, enter:

```
gssm1.example.com(config-gslb-agns[ag-name])# no answer-add
192.168.10.1 name www-zurich-1 order 10
```

Adding Answers to a VIP-Type Answer Group

After you create a VIP-type answer group, add previously configured VIP-type answers to the group using the **answer-add** command in the answer group configuration mode.

The syntax for this command is as follows:

```
answer-add ip_address [name | load-threshold number | order number |
weight number | activate | suspend]
```

The keywords and arguments for this command are as follows:

- ***ip_address***—IP address of a previously configured VIP-type answer. Enter an unquoted text string in dotted decimal format (for example, 192.168.10.1).
- **name**—(Optional) Specifies the name of a previously configured VIP-type answer. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **load-threshold** *number*—(Optional) Assigns the specified load threshold to the answer that is to be added to the answer group. Use this option to determine whether an answer is available, regardless of the balance method type. Valid entries are 2 to 254.
- **order** *number*—(Optional) Assigns the specified order to the answer that is to be added to the answer group. Specify this option when using an ordered balance method type. Valid entries are 0 to 65535.
- **weight** *number*—(Optional) Assigns the specified weight to the answer that is to be added to the answer group. Specify this option when using a weighted round-robin or least-loaded balance method type. Valid entries are 1 to 10.

For more information on the order, weight, and load threshold settings, see the “Balance Methods” section in [Chapter 1, Introducing the Global Site Selector](#).

- **activate**—(Optional) Reactivates a suspended VIP answer. This is the default.
- **suspend**—(Optional) Suspends an active VIP answer.

For example, to add answers to and configure a VIP answer group, enter:

```
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.168.30.1  
name www-hk-1 weight 1  
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.174.20.1  
name www-sf-1 weight 2  
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.188.40.1  
name www-london-1 weight 4  
gssm1.example.com(config-gslb-agvip[ag-name])#
```

To delete an answer from a VIP answer group, enter:

```
gssm1.example.com(config-gslb-agvip[ag-name])# no answer-add  
192.168.30.1 name www-hk-1 weight 1
```

Modifying an Answer Group

Once you create your answer groups, use the CLI in the primary GSSM to make modifications to their configurations, such as adding and removing answers, or changing the order, weight, and load thresholds of the individual answers.

Answers can belong to more than one answer group. However, once you add answers to an answer group, you cannot change the type of an answer group (for example, from VIP to CRA).

To modify an answer group, perform the following steps:

1. Display the current property settings for answer groups by entering the **show gslb-config answer-group** command. See the “[Displaying Answer Group Properties](#)” section for more information.
2. Modify an answer group. Be aware that the commands you use here depend on the changes you need to make. For example, to change the weight assigned to an answer within an answer group, use both the **answer-group** command and the **answer-add** command. To change the owner setting for an answer group, use only the **answer-group** command.
 - For syntax of the **answer-group** command, see the “[Creating an Answer Group](#)” section.
 - For syntax of the **answer-add** command when modifying CRA-type answer groups, see the “[Adding Answers to a CRA-Type Answer Group](#)” section.

- For syntax of the **answer-add** command when modifying NS-type answer groups, see the “[Adding Answers to an NS-Type Answer Group](#)” section.
- For syntax of the **answer-add** command when modifying VIP-type answer groups, see the “[Adding Answers to a VIP-Type Answer Group](#)” section.

For example, to change the order setting for an answer in the VIP answer group ANSGRPVIP4, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP4 owner
WEB-SERVICES type vip
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.168.30.1
name www-hk-1 order 10 comments "CHANGED ORDER 12/01/05"
gssm1.example.com(config-gslb-agvip[ag-name])#
```

To change the owner of the NS answer group ANSGRPNS2, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPNS2 owner
E-COMMERCE type ns
gssm1.example.com(config-gslb-agns[ag-name])#
```

Adding or Deleting an Authority Domain in an Answer Group

Start of Authority (SOA) record TTLs are required when forming negative responses for DNS queries. Be aware that you do not have to configure any SOA records on the GSS to use in the negative response. Instead, you configure a name service (NS) answer on the GSS that specifies the IP address of the authority name server for the domain and the domains hosted on the name server.

To configure as NS answer on the GSS, use the **auth-domain** command in answer group configuration mode. The **no** form of this command deletes an authority domain in an answer group. The syntax of the command is as follows:

```
auth-domain domain-name
no auth-domain domain-name
```



Note

Do not use regular expressions or wild cards with the **auth-domain** command. Use only well-defined domain names.

To add an authority domain, perform the following steps:

1. Configure an NS answer by entering the following commands:

```
gssm1.example.com# config
gssm1.example.com (config)# gslb
gssm1.example.com (config-gslb)# answer ns 1.2.3.4 name ns1
activate
```

2. Configure an answer group and add the NS answer and its associated authority domains by entering the following commands:

```
gssm1.example.com (config-gslb)# answer-group ag1 owner System
type ns
gssm1.example.com (config-gslb-agns)# answer-add 1.2.3.4 name ns1
gssm1.example.com (config-gslb-agns)# auth-domain soa.test
gssm1.example.com (config-gslb-agns)# auth-domain soa.org
```

Upon completion, NS answer 1.2.3.4 is the authoritative name server for the soa.test and soa.org domains, NS 1 answer is the authority for the configured domains soa.test and soa.org, and the GSS is the authority for A record abc.soa.test.

With this configuration, the negative responses for soa.test that need SOA records are included. If there is a cached SOA from answer NS 1, it is used in the negative response. Otherwise, the GSS queries name server ns1 for an SOA record for the domain *soa.test*, uses it in the negative response, and then caches it.

You do not need to configure SOA records on the GSS for the domains for which GSS is authoritative (that is, certain types of resource records). GSS will always obtain the SOA record from the primary name server that is authoritative for the zone.

Suspending or Reactivating All Answers in an Answer Group

You can temporarily stop the GSS from using all answers in an active answer group by modifying the answer group with the **no activate-all-answers** command in answer group configuration mode. When you suspend all answers in an answer group, you prevent that answer group from being used by any of the currently configured DNS rules. Suspending the answers in one answer group also affects any other answer groups to which those answers belong.

To reactivate the answers in the answer group, use the **activate-all-answers** command in the answer group configuration mode for a specific answer group.

To suspend all answers in an answer group, perform the following steps:

1. Display the current answer groups by entering the **show gslb-config answer-group** command. See the “[Displaying Answer Group Properties](#)” section for more information.
2. Identify the active answer group that you want to suspend, and then use the **answer-group** command and the **no activate-all-answers** command to suspend all answers in the group.

For example, to suspend all answers in the vip-type answer group ANSGRPVIP4, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP4 owner
WEB-SERVICES type vip
gssm1.example.com(config-gslb-agvip[ag-name])# no
activate-all-answers
gssm1.example.com(config-gslb-agvip[ag-name])#
```

To reactivate all answers in a suspended answer group, use the **activate-all-answers** command.

For example, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP4 owner
WEB-SERVICES type vip
gssm1.example.com(config-gslb-agvip[ag-name])# activate-all-answers
gssm1.example.com(config-gslb-agvip[ag-name])#
```

Suspending or Reactivating an Answer in an Answer Group

You can temporarily stop the GSS from using an answer in an active answer group by modifying the answer group with the **suspend** keyword in the **answer-add** command. Enter this command in answer group configuration mode. Suspending prevents that answer in the answer group from being used by any of the currently configured DNS rules.



Note

Suspending an answer in one answer group also affects any other answer groups to which the answer belongs.

To reactivate an answer in the answer group, use the **active** option (for the **answer-add** command) in the answer group configuration mode.

To suspend an answer in an answer group, perform the following steps:

1. Display the current answers and answer groups by entering the **show gslb-config answer-group** command. See the “[Displaying Answer Group Properties](#)” section for more information.
2. Identify the active answer that you want to suspend (and its answer group), and then use the **answer-add** command and the **suspend** option to suspend the answer in the group.

For example, to suspend the answer `www-sf-1` in the `vip-type` answer group `ANSGRPVIP4`, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP4 owner  
WEB-SERVICES type vip  
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.168.30.1  
suspend  
gssm1.example.com(config-gslb-agvip[ag-name])#
```

For example, to reactivate a suspended answer in an answer group with the **activate** command, enter:

```
gssm1.example.com(config-gslb)# answer-group ANSGRPVIP4 owner  
WEB-SERVICES type vip  
gssm1.example.com(config-gslb-agvip[ag-name])# answer-add 192.168.30.1  
activate  
gssm1.example.com(config-gslb-agvip[ag-name])#
```

Suspending or Reactivating All Answers in Answer Groups Associated with an Owner

You can group and manage answers added to answer groups according to the GSS owner. Using a GSS owner to manage your answer groups enables you to quickly suspend or activate related answers.

To suspend or reactivate all answers in answer groups associated with a GSS owner, use the **suspend-all-answers** and **activate-all-answers** keywords (for the **owner** command).

To display the currently configured owners, answers, and answer groups, use the **show gslb-config answer-group** command.

For example, to suspend all answers in answer groups associated with the owner `WEB-SERVICES`, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# owner WEB-SERVICES suspend-all-answers
gssm1.example.com(config-gslb)#
```

To reactivate all answers in answer groups associated with the owner WEB-SERVICES, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# owner WEB-SERVICES
activate-all-answers
gssm1.example.com(config-gslb)#
```

Displaying Answer Group Properties

You can display the current property settings for all answer groups by entering the **show gslb-config answer-group** command.

The syntax of this command is as follows:

```
show gslb-config answer-group
```

For example, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer-group
...
answer-group AGROUP1 owner "OWNER1" type ns
answer-group AGROUP2 owner "OWNER2" type cra
answer-group AGROUP3 owner System type vip
...
```

To display the properties for an answer group based on an answer group name, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer-group ANGROUP1

answer-group AGROUP1 owner "OWNER1" type ns
```

Deleting an Answer Group



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

Before deleting an answer group, verify that none of your DNS rules reference the answer group that you are about to delete. If necessary, deselect the answer group from the DNS rule. See [Chapter 7, Building and Modifying DNS Rules](#), for information about modifying a DNS rule.

Deleting an answer group does not delete the answers contained in the answer group.

To delete an answer group, perform the following steps:

1. Display the current answers by entering the **show gslb-config answer-group** command. See the “[Displaying Answer Group Properties](#)” section for more information.
2. Identify the active answer group that you want to delete, and then use the **no** form of the **answer-group** command to delete the answer.

For example, to delete the VIP-type answer group ANSGRPVIP1, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer-group
```

```
answer-group ANSGRPVIP1 owner OWNr1 type vip  
answer-group ANSGRPVIP2 owner System type vip
```

```
gssm1.example.com(config-gslb)# no answer-group ANSGRPVIP1  
gssm1.example.com(config-gslb)#
```

Where to Go Next

[Chapter 7, Building and Modifying DNS Rules](#), describes how to construct the DNS rules that govern all global server load balancing on your GSS network.

Where to Go Next



Building and Modifying DNS Rules

This chapter describes how to build and modify Domain Name System (DNS) rules on your GSS network. After you configure your source address lists, domain lists, answers, and answer groups, you are ready to begin constructing the DNS rules that will control global server load balancing on your GSS network.

When building DNS rules, you specify the actions for the GSS to perform when it receives a request from a known source (a member of a source address list) for a known hosted domain (a member of a domain list). The DNS rule specifies which response (answer) is given to the requesting user's local DNS host (D-proxy) and how that answer is chosen. The GSS uses one of a variety of balance methods to determine the best response to the request, which is based on the status and load of your GSS host devices.

**Note**

Before you create DNS rules, review the “[GSS Architecture](#)” section in [Chapter 1, Introducing the Global Site Selector](#).

This chapter contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Building DNS Rules](#)
- [Modifying DNS Rules and Balance Clauses](#)
- [Displaying DNS Rule Properties](#)
- [Suspending a DNS Rule](#)
- [Reactivating a DNS Rule](#)
- [Suspending or Reactivating All DNS Rules Belonging to an Owner](#)

- [Deleting a DNS Rule](#)
- [Configuring DNS Rule Filters](#)
- [Removing DNS Rule Filters](#)
- [Delegating to GSS Devices](#)
- [Where To Go Next](#)

Logging in to the CLI and Enabling Privileged EXEC Mode



Note

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Building DNS Rules

You can build the DNS rules that specify the actions that each GSS is to perform when it receives a request from a known source for a known hosted domain. Do so by entering the **dns rule** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
dns rule name { owner name | source-address-list name | domain-list name
| query { a | all }
```



Note

After you enter the **dns rule** *name* command, the prompt changes to the rule configuration mode where you specify and configure load-balance clauses and optional DNS sticky and network proximity settings.

The keywords and arguments for this command are as follows:

- **name**—Name for the DNS rule. Enter a unique alphanumeric name with a maximum of 80 characters. Names should not contain spaces.
- **owner name**—Specifies the name of a previously created owner with whom the rule will be associated. The default owner is System.
- **source-address-list name**—Specifies the name of a previously created source address list from which requests will originate. The DNS rule is applied only to requests coming from one of the addresses in the source address list. If you do not choose a source address list, the GSS automatically uses the default list Anywhere.
- **domain-list name**—Specifies the name of a previously created domain list to which DNS queries will be addressed. The DNS rule is applied only to requests coming from one of the addresses in the source address list and for a domain on the specified domain list.
- **query**—Specifies the type of DNS query to apply to the rule. Choose one of the following:
 - **a** —The DNS rule is applied only to answer address record (A-record) requests originating from a host on the configured source address list. Any requests with unsupported query types (for example, MX, PTR, or CNAME records) that match this DNS rule are dropped and not answered

by the GSS. For an AAAA query with a configured host domain, the GSS returns a NODATA (No Answer, No Error) response for the requester to make a subsequent A-record query.

- **All**—The DNS rule is applied to all DNS queries originating from a host on the configured source address list. For any request other than an A-record query (for example, MX or CNAME record), the GSS forwards the request to a name server configured in one of the three balance clauses. When the GSS receives the response from the name server, it delivers the response to the requesting client D-proxy.

**Note**

When you select **All**, you must configure one balance clause to include a name server-type answer group.

For example, to create a DNS rule called drule02, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# dns rule drule02 owner WEB-SERVICES
source-address-list WEB-GLOBAL-LISTS domain-list E-COMMERCE query a
gssm1.example.com(config-gslb-rule[rule-name])#
```

To delete a DNS rule called drule02, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no dns rule drule02 owner WEB-SERVICES
source-address-list WEB-GLOBAL-LISTS domain-list E-COMMERCE query a
```

Configuring Balance Clauses for a DNS Rule

After you create a DNS rule, you configure the balance clauses used by the rule by specifying the answer group and balance method that make up each balance clause. In addition, you can configure optional DNS sticky and network proximity settings. If you intend to use DNS sticky or network proximity, see [Chapter 8, Configuring DNS Sticky](#) or [Chapter 9, Configuring Network Proximity](#) for the configuration procedures.

The GSS can use a maximum of three possible balance method clauses in a DNS rule to select the most appropriate resource to serve a user request. Each balance method provides a different algorithm for selecting one answer from a configured answer group. Each clause specifies that a particular answer group serve the request and a specific balance method be used to select the best resource from that answer group.

The balance clauses that you configure in a DNS rule are evaluated in order, with parameters established to determine when a clause is skipped and the next clause used. A balance clause is skipped when any one of the following conditions exists:

- A least-loaded balance method is selected and the load threshold for all online answers is exceeded.
- The VIP answers in the specified VIP answer group are offline.
- Proximity is enabled for a VIP-type answer group and the DRP agents do not return any RTT values that meet the value set for **acceptable-rtt**.
- All answers in a CRA- or NS-type answer group are offline and keepalives are enabled to monitor the answers.

To create balance clauses for a DNS rule, you use the **clause** command in the rule configuration mode. The syntax for this command is as follows:

```
clause number { cra-group name | ns-group name | vip-group name }
```

The keywords and arguments for this command are as follows:

- *number*—Balance clause number (**1**, **2**, or **3**). For clauses that use VIP- or NS-type answer groups, you can specify **1**, **2**, or **3**. For clauses that use CRA-type answer groups, you can specify only **1** or **2**.
- **cra-group** *name*—Specifies that the balance clause is to use a CRA-type answer group. Enter the name of a previously created CRA-type answer group.
- **ns-group** *name*—Specifies that the balance clause is to use an NS-type answer group. Enter the name of a previously created NS-type answer group.
- **vip-group** *name*—Specifies that the balance clause is to use a VIP-type answer group. Enter the name of a previously created VIP-type answer group.

The answer group type (VIP, NS, or CRA) that you select for your balance clause determines the keywords and arguments that appear in the CLI.

This section contains the following topics:

- [Configuring Balance Clauses that Use VIP-Type Answer Groups](#)
- [Configuring Balance Clauses that Use NS-Type Answer Groups](#)
- [Configuring Balance Clauses that Use CRA-Type Answer Groups](#)

Configuring Balance Clauses that Use VIP-Type Answer Groups

You can create balance clauses for a DNS rule that use VIP-type answer groups by entering the **clause number vip-group name** command in the rule configuration mode.

The syntax for this command is as follows:

```
clause number vip-group name [method { round-robin | least-loaded | ordered | weighted-round-robin | hashed { domain-name | source-address | both } } [count number | tll number]]
```

The keywords and arguments for this command are as follows:

- *number*—Balance clause number (**1**, **2**, or **3**). You can specify a maximum of three balance clauses that use VIP-type answers.
- **vip-group name**—Specifies the name of a previously created VIP-type answer group.
- **method**—(Optional) Specifies the method type for each balance clause. Method types are as follows:
 - **round-robin**—The GSS cycles through the list of answers that are available as requests are received. This is the default.
 - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request. The least-loaded option is available only for VIP-type answer groups that use a KAL-AP keepalive.
 - **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports gaps in numbering in an ordered list.



Note

For answers that have the same order number in an answer group, the GSS will use only the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

- **weighted-round-robin**—The GSS cycles through the list of answers that are available as the requests are received, but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.
- **hashed**—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group as follows:
 - **source-address**—The GSS selects the answer based on a hash value created from the source address of the request.
 - **domain-name**—The GSS selects the answer based on a hash value created from the requested domain name.
 - **both**—The GSS selects the answer based on both the source address and domain name.
- **count number**—(Optional) Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule. The default is 1 record.
- **tll number**—(Optional) Specifies the duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer. Valid entries are 0 to 604,800 seconds. The default is 20 seconds.

For example, to configure a balance clause for a DNS rule, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group  
ANSGRP-VIP-01 method ordered tll 60
```

**Note**

If you configured a DNS rule with a balance clause that uses a CRA-type answer group, you must immediately follow the CRA-type clause with a balance clause that uses a VIP-type answer group. This ensures that if none of the Content Routing Agents successfully respond to the DNS race request, a “last gasp” server response from the VIP-type balance clause is sent to the requesting name server.

To reset the balance clause settings to their defaults for the DNS rule, use the **no** form of the **clause** command. For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# no clause 1 vip-group  
ANSGRP-VIP-01 method ordered tll 60
```

You can create a maximum of three balance clauses that use VIP-type answer groups. A second or third balance clause applies only when the preceding clause is unable to provide an answer for the DNS query.

**Note**

If you plan to configure DNS sticky in the DNS rule, see [Chapter 8, Configuring DNS Sticky](#). If you plan to configure network proximity in the DNS rule, see [Chapter 9, Configuring Network Proximity](#).

Configuring Balance Clauses that Use NS-Type Answer Groups

You can create balance clauses for a DNS rule that uses NS-type answer groups by using the **clause number ns-group name** command in the rule configuration mode.

The syntax for this command is as follows:

```
clause number ns-group name [method { round-robin | least-loaded |
ordered | weighted-round-robin | hashed { domain-name | source-address
| both } } ]
```

The keywords and arguments for this command are as follows:

- **number**—Balance clause number (**1**, **2**, or **3**). You can specify a maximum of three balance clauses that use NS-type answers.
- **ns-group name**—Specifies the name of a previously created ns-type answer group.
- **method**—Specifies the method type for each of your balance clauses. Method types are as follows:
 - **round-robin**—The GSS cycles through the list of answers that are available as requests are received. This is the default.
 - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request. The least-loaded option is available only for VIP-type answer groups that use a KAL-AP keepalive.
 - **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports gaps in numbering in an ordered list.



Note For answers that have the same order number in an answer group, the GSS will only use the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

- **weighted-round-robin**—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.
- **hashed**—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group as follows:
 - **domain-name**—The GSS selects the answer based on a hash value created from the requested domain name.
 - **source-address**—The GSS selects the answer based on a hash value created from the source address of the request.
 - **both**—The GSS selects the answer based on both the source-address and domain name.

For example, to configure a balance clause for the DNS rule, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 ns-group  
ANSGRP-NS-01 method hashed both
```

To reset the balance clause settings for the DNS rule to their defaults, use the **no** form of the **clause** command. For example:

```
gssm1.example.com(config-gslb-rule[rule-name])# no clause 1 ns-group  
ANSGRP-NS-01 method hashed both
```

You can create a maximum of three balance clauses that use NS-type answer groups. A second or third balance clause applies only when the preceding clause is unable to provide an answer for the DNS query.

Configuring Balance Clauses that Use CRA-Type Answer Groups

You can create balance clauses for a DNS rule that use CRA-type answer groups by using the **clause number cra-group name** command in the rule configuration mode.

The syntax for this command is as follows:

```
clause number cra-group name [method boomerang | fragment number |  
ip-ttl number | max-prop-delaynumber | pad number | secret key |  
server-delay number | ttl number]
```

The keywords and arguments for this command are as follows:

- *number*—Balance clause number (**1** or **2**). You can specify a maximum of two balance clauses that use CRA-type answers.
- **cra-group name**—Specifies the name of a previously created CRA-type answer group.
- **method boomerang**—Specifies that the balance method uses the boomerang DNS race to determine the best site. See the “[DNS Race \(Boomerang\) Method](#)” section in [Chapter 1, Introducing the Global Site Selector](#), for more information on this balance method type. This is the default setting and cannot be changed.
- **fragment number**—(Optional) Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule. The default is 1 record.
- **ip-ttl number**—(Optional) Specifies the maximum number of network hops that should be used when returning a response to a CRA from a match on a DNS rule.
- **max-prop-delay**number—(Optional) Specifies the maximum propagation delay, which is the maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS forwards a DNS request to a CRA.
- **pad number**—(Optional) Specifies the amount of extra data (in bytes) included with each CRA response packet that is used to evaluate CRA bandwidth and latency when making load-balancing decisions.
- **secret key**—(Optional) Specifies a text string with a maximum of 64 characters used to encrypt critical data sent between the GSS boomerang server and CRAs. This key must be the same for each configured CRA.

- **server-delay number**—(Optional) Specifies the maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS returns the address of its “last gasp” server as a response to the requesting name server.
- **ttl number**—(Optional) Specifies the duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer. Valid entries are 0 to 604,800 seconds. The default is 20 seconds.

For example, to configure a balance clause for the DNS rule, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 cra-group  
ANSGRP-CRA-01 fragment 2 pad 20
```

**Note**

Always follow a balance clause that uses a CRA-type answer group with a balance clause that uses a VIP-type answer group. This ensures that if none of the Content Routing Agents successfully respond to the DNS race request, a “last gasp” server response from the VIP-type balance clause is sent to the requesting name server.

To reset the balance clause settings for the DNS rule to their defaults, use the **no** form of the **clause** command. For example:

```
gssm1.example.com(config-gslb-rule[rule-name])# no clause 1 cra-group  
ANSGRP-CRA-01 fragment 2 pad 20
```

You can create a maximum of two balance clauses that use CRA-type answer groups. A second balance clause applies only when the first clause is unable to provide an answer for the DNS query.

Modifying DNS Rules and Balance Clauses

You can use the CLI to modify properties for an existing DNS rule or the balance clauses within a DNS rule. This section contains the following topics:

- [Modifying DNS Rule Properties](#)
- [Modifying Balance Clause Properties](#)

Modifying DNS Rule Properties

To modify an existing DNS rule, perform the following steps:

1. Display the current property settings for a DNS rule by entering the **show gslb-config dns rule *name*** command. See the “[Displaying DNS Rule Properties](#)” section for more information.
2. Change the settings for a DNS rule by entering the **dns rule *name*** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
dns rule name {owner name | source-address-list name | domain-list name | query {a | all}}:
```

See the “[Building DNS Rules](#)” section for details about the keywords and arguments for this command.

3. Make modifications as necessary to the DNS rule options.

For example, to change the domain list for an existing DNS rule named drule02, enter:

```
gssm1.example.com(config-gslb)# show gslb-config dns rule drule02

dns rule drule02  owner WEB-SERVICES source-address-list
WEB-GLOBAL-LISTS domain-list E-COMMERCE query a
clause 1 vip-group ANSGRP6 least-loaded ttl 20 count 2 sticky disable

gssm1.example.com(config-gslb)# dns rule drule02 owner WEB-SERVICES
source-address-list WEB-GLOBAL LISTS domain-list SECURITY query a
gssm1.example.com(config-gslb-rule[rule-name])#
```

Modifying Balance Clause Properties

To modify balance clause properties for an existing DNS rule using the CLI, perform the following steps:

1. Display the current property settings for a DNS rule and the balance clauses for that rule by entering the **show gslb-config dns rule** *name* command. See the “[Displaying DNS Rule Properties](#)” section for more information.
2. Change the balance clause properties for an existing DNS rule by using the **dns rule** *name* command in global server load-balancing configuration mode. This command allows you to access the rule configuration mode for the desired rule.

For example, enter:

```
gssml.example.com(config-gslb)# dns rule drule02
gssml.example.com(config-gslb-rule[rule-name])#
```

3. Modify balance clause properties by using the **clause** command. The syntax of the clause command varies according to the answer group type (VIP, CRA, or NS) that it uses. See the following sections for **clause** command syntax based on answer group type:
 - [Configuring Balance Clauses that Use VIP-Type Answer Groups](#)
 - [Configuring Balance Clauses that Use NS-Type Answer Groups](#)
 - [Configuring Balance Clauses that Use CRA-Type Answer Groups](#)
4. Make modifications as necessary to the balance clause keywords and arguments.

For example, to change the method type for clause 1 of the DNS rule drule02 from least-loaded to round-robin, enter:

```
gssml.example.com(config-gslb)# show gslb-config dns rule drule02

dns rule drule02  owner WEB-SERVICES source-address-list
WEB-GLOBAL-LISTS domain-list E-COMMERCE query  a
clause 1 vip-group ANSGRP6 least-loaded  ttl 20 count 2 sticky disable

gssml.example.com(config-gslb)# dns rule drule02
gssml.example.com(config-gslb-rule[rule-name])# clause 1 vip-group
ANSGRP6 method round-robin ttl 20 count 2
```

Displaying DNS Rule Properties

You can use the **show gslb-config dns rule** command to display the current property settings for all DNS rules and balance clauses for each rule.

The syntax of this command is as follows:

```
show gslb-config dns rule [name]
```

The optional *name* argument specifies the name of a previously created DNS rule.

For example, to display the properties for the DNS rule drule02, enter:

```
gssm1.example.com(config-gslb)# show gslb-config dns rule drule02

dns rule drule02  owner WEB-SERVICES source-address-list
WEB-GLOBAL-LISTS domain-list E-COMMERCE query a
clause 1 vip-group ANSGRP6 least-loaded  ttl 20 count 2 sticky disable

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

Suspending a DNS Rule

If you want to stop requests from being processed by a DNS rule on your GSS, log in to the primary GSSM GUI and access the **DNS Rules** tab. See the “Suspending a DNS Rule,” section in Chapter 7, Building and Modifying DNS Rules, in the *Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide* for details.

Reactivating a DNS Rule

If you want to reactivate the operation of a suspended DNS rule on your GSS, log in to the primary GSSM GUI and access the **DNS Rules** tab. See the “Reactivating a DNS Rule,” section in Chapter 7, Building and Modifying DNS Rules, in the *Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide* for details.

Suspending or Reactivating All DNS Rules Belonging to an Owner

You can group and manage your DNS rules according to an established GSS owner. Using a GSS owner to manage your DNS rules enables you to quickly suspend or activate all rules related to a particular group or department within your organization (for example, HR or Sales) without individually editing each rule that serves that owner.

To suspend or reactivate all DSN rules associated with a GSS owner, use the **owner** command with the **suspend-all-rules** and **activate-all-rules** keywords.

To display the currently configured DNS rules and their associated owners, use the **show gslb-config dns rule** command. See the “[Displaying DNS Rule Properties](#)” section for more information.

For example, to suspend all DNS rules associated with the owner WEB-SERVICES, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# owner WEB-SERVICES suspend-all-rules  
gssm1.example.com(config-gslb)#
```

To reactivate all DNS rules associated with the owner WEB-SERVICES, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# owner WEB-SERVICES activate-all-rules  
gssm1.example.com(config-gslb)#
```

Deleting a DNS Rule

You can use the **no** form of the **dns rule** command to remove a previously created DNS rule from the GSSM database. Deleting a DNS rule does not delete the source address lists, domain lists, owners, and answer groups associated with the DNS rule.



Caution

Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. See the *Global Site Selector Administration Guide* for details.

To delete a DNS rule, perform the following steps:

1. Display the current DNS rules by using the **show gslb-config dns rule** command. See the [Displaying DNS Rule Properties](#) section for more information.
2. Identify the DNS rule that you want to delete, and then use the **no** form of the **dns rule** command to delete the rule.

For example, to delete a DNS rule named RULE1, enter:

```
gssm1.example.com(config-gslb)# show gslb-config dns rule
...
dns rule RULE1 owner OWNER1 source-address-list Anywhere domain-list
www.wonderland.com query a
      clause 1 vip-group ans-grp1 method ordered ttl 20 count 1 sticky
disable
...
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no dns rule RULE1 owner OWNER1
source-address-list ANYWHERE domain-list WWW.WONDERLAND.COM query A
gssm1.example.com(config-gslb)#
```

Configuring DNS Rule Filters

If you want to configure DNS rule filters on your GSS, log in to the primary GSSM GUI and access the **DNS Rules** tab. See the “Configuring DNS Rule Filters,” section in Chapter 7, Building and Modifying DNS Rules, in the *Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide* for details.

Removing DNS Rule Filters

If you want to remove DNS rule filters on your GSS, log in to the primary GSSM GUI and access the **DNS Rules** tab. See the “Removing DNS Rule Filters,” section in Chapter 7, Building and Modifying DNS Rules, in the *Cisco Global Site Selector GUI-Based Global Server Load-Balancing Configuration Guide* for details.

Delegating to GSS Devices

After you configure your GSS devices to connect to your network and create the logical resources (source address lists, domain lists, answers and answer groups, and DNS rules) required for global server load balancing, you can integrate your global server load-balancing device into your network’s DNS infrastructure to deliver user queries to your GSS. To accomplish this integration, you must modify your parent domain’s DNS server to delegate parts of its name space to your GSS devices.

You should carefully review and perform a test of your GSS deployment before making changes to your DNS server configuration that will affect your public or enterprise network configuration.

Modifying your DNS servers to accommodate your GSS devices involves the following steps:

1. Adding name server (NS) records to your DNS zone configuration file that delegates your domain or subdomains to one or more of your GSSs.
2. Adding “glue” address (A) records to your DNS zone configuration file that map the DNS name of each of your GSS devices to an IP address.

**Note**

The A-records which define the name servers within the domain are frequently called glue records.

[Example 7-1](#) provides an example of a DNS zone configuration file for a fictitious cisco.com domain that has been modified to delegate primary DNS authority for three domains to two GSS devices. Relevant lines are shown in bold type.

In [Example 7-1](#), the delegated domains are as follows:

- www.cisco.com
- ftp.cisco.com
- media.cisco.com

The GSS devices are as follows:

- gss1.cisco.com
- gss2.cisco.com

Example 7-1 Sample BIND Zone Configuration File Delegating GSSs

```
cisco.com. IN SOA ns1.cisco.com. postmaster.cisco.com. (
    2001111001; serial number
    36000; refresh 10 hours
    3600 ; retry 1 hour
    3600000; expire 42 days
    360000; minimum 100 hours )

; Corporate Name Servers for cisco.com
    IN NS ns1.cisco.com.
    IN NS ns2.cisco.com.
ns1    IN A 192.168.157.209
ns2    IN A 192.168.150.100

; Sub-domains delegated to GSS Network
www    IN NS gss1.cisco.com.
        IN NS gss2.cisco.com.
media  IN CNAME www
ftp    IN NS gss1.cisco.com.
        IN NS gss2.cisco.com.
```

```
; "Glue" A records with GSS interface addresses
;      Cisco GSS Dallas
gss1  IN  A   172.16.2.3
;      Cisco GSS London
gss2  IN  A   192.168.3.6
.
.
```

You can use many possible GSS deployments when reviewing this zone file; some deployments may suit your needs and your network better than the previous example. For example, instead of having all subdomains shared by all GSS devices, you may want to allocate specific subdomains to specific GSSs.

Where To Go Next

If you plan to use DNS sticky for your global server load balancing, configure local or global DNS sticky for GSS devices in your network. See [Chapter 8, Configuring DNS Sticky](#), for details.

If you plan to use network proximity for your global server load balancing, configure proximity for GSS devices in your network. See [Chapter 9, Configuring Network Proximity](#), for details.

Where To Go Next



Configuring DNS Sticky

This chapter describes how to configure a GSS to support Domain Name System (DNS) stickiness to answer requests received from client D-proxies. The GSS supports DNS sticky both locally and globally between GSS network peers.

This chapter contains the following major sections:

- [DNS Sticky Overview](#)
- [DNS Sticky Quick Start Guide](#)
- [Synchronizing the GSS System Clock with an NTP Server](#)
- [Configuring Sticky Using the Primary GSSM CLI](#)
- [Disabling DNS Sticky Locally on a GSS for Troubleshooting](#)

Each GSS supports a comprehensive set of **show** CLI commands to display sticky application mesh statistics for the GSS device. In addition, the primary GSSM GUI displays sticky statistics for the GSS network. See [Chapter 13, Displaying GSS Global Server Load-Balancing Statistics](#), for details about viewing sticky statistics.

DNS Sticky Overview

Stickiness, also known as persistent answers or answer caching, enables a GSS to remember the DNS response returned for a client D-proxy and to later return that same answer when the client D-proxy makes the same request. When you enable stickiness in a DNS rule, the GSS makes a best effort to always provide identical A-record responses to the requesting client D-proxy, assuming that the original Virtual IP address (VIP) continues to be available.

For many users browsing a site, being redirected to a new site is transparent. However, customers performing e-commerce or other transactions may experience a break in the connection when redirected, which results in a loss of the e-commerce transaction. Having DNS sticky enabled on a GSS helps to ensure that e-commerce clients remain connected to a particular server for the duration of a transaction, even when the client's browser refreshes the DNS mapping.

While some browsers allow client connections to remain for the lifetime of the browser instance or for several hours, other browsers may impose a connection limit of 30 minutes before requiring a DNS re-resolution. This time period may not be long enough for a client to complete an e-commerce transaction. A new DNS resolution can then cause the client to connect to a server that is different from the original server, disrupting the transaction. DNS sticky helps to ensure that a client completes a transaction if a DNS re-resolution occurs.

This section contains the following topics on DNS sticky in the GSS:

- [Local DNS Sticky](#)
- [Sticky Database](#)
- [Global DNS Sticky](#)

Local DNS Sticky

With local DNS sticky, each GSS device attempts to ensure that subsequent client D-proxy requests to the same domain name from the same GSS device will be “stuck” to the same location as the first request. DNS sticky guarantees that all requests from a client D-proxy to a particular hosted domain or domain list are given the same answer by the GSS for the duration of a user-configurable sticky inactivity time interval, assuming the answer is still valid.

Each GSS dynamically builds and maintains a local sticky database that is based on the answers that the GSS sends to the requesting client D-proxies. If a subsequent request comes from the same client D-proxy, and the answer in the database is valid, the GSS returns the cached answer to the client D-proxy.

You configure the GSS to perform sticky load-balancing operations by configuring options on DNS rules and balance clauses. You identify the sticky method used by the DNS rule by matching a hosted domain or matching a hosted domain list. When sticking on a domain, the GSS provides the same sticky answer to all requests from a client D-proxy for that domain. When sticking on a domain list, the GSS provides the same sticky answer to all requests from a client D-proxy for all domains in that domain list.

Before returning a sticky answer to a client, the GSS verifies the keepalive status. If the resource is:

- Available (online state), the GSS uses this answer for the DNS response sent back to the D-proxy.
- Available (online state) but the VIP corresponding to the answer is overloaded, the GSS continues to use this answer for the DNS response sent back to the D-proxy. Sticky always takes precedence over an exceeded load threshold in the associated DNS rule.
- Unavailable (offline state), the GSS selects a new answer and inserts this answer into the sticky database, replacing the previous answer.

Sticky Database

The sticky database provides the core intelligence for all DNS sticky-based decisions made by a GSS, on a local or global level. The GSS collects requests from the client D-proxies and stores these requests in memory as the sticky database. Requests may be identified by the IP address of the client D-proxy or a database ID representing a list of D-proxy IP addresses (configured as a sticky group, see the [“Creating Sticky Groups”](#) section). The D-proxy IP address may also be some form of a sticky global netmask if the global subnet mask is set to a value other than the default of 255.255.255.255.

The sticky database stores the answer to each request that the DNS rule matches, which may be for a single domain (including wildcard expressions) or a configured list of domains. These components comprise each sticky database key that the GSS uses for the lookup, storage, and persistence of stickiness for DNS responses.

The primary GSSM supports the creation of sticky groups that allow you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its sticky database as a single entry. Instead of multiple sticky database entries, the GSS uses only one entry in the sticky database for multiple D-proxies. The GSS treats all D-proxies in a sticky group as a single D-proxy.

All entries in the sticky database age out based on a user-specified global sticky inactivity timeout value. The sticky inactivity timeout value identifies the time period that an answer remains valid in the sticky database. Every time the GSS returns an answer to the requesting client, the GSS resets the expiration time of the answer to this value. When the sticky inactivity timeout value elapses without the client requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. You can specify a global sticky inactivity timeout default value for the GSS or modify the inactivity timeout value for each DNS rule.

**Note**

The sticky inactivity timeout is accurate to within 5 minutes of the specified value. Each entry persists in the sticky database for the configured sticky inactivity timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

Upon receiving a DNS request, the GSS searches the sticky database for a matched entry based on the combination of D-proxy IP address (or sticky group ID) and requested hosted domain or domain list information in the request. If the GSS finds a matched entry (a hit), the GSS returns the original DNS answer to the requesting D-proxy and the GSS resets the user-configured sticky inactivity timeout to its starting value. If the GSS does not find a matched entry (a miss), the GSS does not return a sticky answer but, instead, performs normal load balancing for the request to locate a new answer and add the new entry into the sticky database.

The GSS supports a maximum of 400,000 entries in the sticky database. When the total number of entries in the sticky database reaches 400,000, the GSS automatically removes entries from the database based on the lowest percentage of time remaining.

Global DNS Sticky

This section provides an overview of the global DNS sticky function and the behavior of GSS devices operating in a peer mesh. It contains the following topics:

- [GSS Sticky Peer Mesh](#)
- [Sticky Mesh Conflict Resolution](#)
- [Communicating in the Sticky Peer Mesh](#)

GSS Sticky Peer Mesh

With global DNS sticky enabled, each GSS device in the network shares sticky database answers with the other GSS devices in the network, operating as a fully connected peer-to-peer mesh. Each GSS device in the mesh stores the requests and responses from client D-proxies in its own local database and shares this information with the other GSS devices in the network. Subsequent client D-proxy requests to the same domain name to any GSS in the network cause the client to be “stuck.”

When one GSS device in the mesh receives a query from a client for a hosted domain or domain list, global sticky enables each GSS in the network to make a best effort attempt to return the same answer to the requesting client. This action is performed regardless of which GSS in the network is selected to answer the first and subsequent requests. The individual GSS devices work together to maintain a global sticky database across the network.

Each GSS in the peer mesh receives updates from the other peers and sends local changes to its remote peers. The GSS devices share the following information with the other GSS devices in the peer mesh:

- The sticky database lookups performed
- The persistent answers provided in the response
- The related time stamp and sticky inactivity timeout details

Each GSS sends updates to its remote GSS peers when any of the following events occur:

- A D-proxy request arrives at a GSS with no previous database entry. The GSS returns a new answer to the requesting client and enters that answer in its local database.
- A GSS returns a previous answer to the requesting client. The GSS resets the expiration time for the answer to its original sticky inactivity timeout value.
- The GSS finds an existing answer in the sticky database but a keepalive determines that the answer is nonresponsive (offline). In this case, the GSS uses the DNS rule to choose a new answer, overriding the previous answer in the sticky database, and communicates this answer to all peers.
- You use the **sticky database delete** CLI command to delete one or more entries from the sticky database.

A GSS does not send information to its peers when it purges an answer from the sticky database when reaching the normal sticky inactivity timeout or a sticky database overflow. Each GSS in the mesh is expected to perform this task independently.

When a local GSS node receives information from one of its peers in the network, that GSS performs a lookup of each received data entry in its local sticky database. Based on the results of the lookup, the GSS performs one of the following actions:

- If the GSS does not find the entry in its sticky database, the GSS adds the answer to its local sticky database.
- If the GSS finds the same entry in its sticky database, the GSS resets the expiration time for the answer to the initial sticky inactivity timeout value.

The GSS supports encryption of all inter-GSS communications to maintain the integrity of the sticky database information transferred among the mesh peers. Each GSS uses the Message Digest 5 (MD5)-based hashing method to encrypt the application data sent throughout the mesh.

To authenticate communication between GSS devices in the mesh to prevent unauthorized device access, you can specify a secret string that is used by all GSS devices in the mesh. The secret string provides a key for authentication between GSS devices as well as for encryption (if enabled). Each local GSS uses the Challenge Handshake Authentication Protocol (CHAP) method to establish a connection with a remote peer.

Sticky Mesh Conflict Resolution

In some instances, two or more GSS devices in the mesh may answer the same sticky request at the same time. When GSS devices communicate their updates to each peer, the recipient detects a conflict. Conflicts are resolved in the peer network by each GSS that keeps the record of the entry with the greatest expiration time stamp, (that is, the newest record). If the conflicting entries have identical time stamps, the GSS uses the entry that contains the most recently configured answer based on the configuration ID.

Conflicts are far more likely to occur when multiple requests are grouped by domain list, or when you group D-proxy clients by a sticky mask or by sticky group. For example, if you configure a DNS rule for domains A and B, one client may request GSS 1 for domain A, while a second client may make a request for domain B. If the GSS receives both requests at the same time, the two clients may receive different answers.

You can reduce global sticky mesh conflicts as follows:

- Configure sticky DNS rules for one domain only. Avoid using the **domain-list** option for the sticky method unless absolutely necessary.
- Avoid using domain wildcards. Wildcard domains pose the same issue as domain lists.
- Avoid using low DNS **ttl** values in a sticky balance clause. Setting the **ttl** value of each sticky balance clause to a high value allows the sticky database to synchronize answers before the client D-proxy attempts to re-resolve the answer.

Communicating in the Sticky Peer Mesh

You can successfully pass packets between GSS peers in the sticky mesh by ensuring that the following requirements are met:

- Synchronize the system clock of each GSS device in the mesh with a Network Time Protocol (NTP) server. If a GSS system clock is out of synchronization with the other GSS peers (by a value greater than 3 minutes), that GSS ignores update messages from other GSS devices until you synchronize its system clock. See the [“Synchronizing the GSS System Clock with an NTP Server”](#) section for details.

- Each GSS in the peer mesh has the same global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change were made on the primary GSSM and the peer did not receive the change due to a network failure. See the [“Configuring DNS Sticky”](#) section for details.
- Each GSS in the peer mesh has the same GSS software version.

If these conditions are not met, a GSS cannot properly receive or send packets with the other GSS peers in the sticky mesh.

A GSS leaves and rejoins the global sticky mesh when you perform one of the following actions:

- Enter the **gss restart** command to restart the GSS software on the local GSS node.
- Enter the **sticky stop** and **sticky start** command sequence on the local GSS node.
- Enter the **reload** command to perform a cold restart of the local GSS node.
- Enter the **enable global** command in sticky properties configuration mode.

Upon reentry into the mesh, the GSS attempts to load the sticky database from a peer GSS. The GSS uses the shortest round-trip time (RTT) to prioritize from which peer to request the database update. If a GSS peer is unavailable, the GSS locally restores the sticky database from the last available periodic database dump file. The GSS restores the sticky database from the database dump file any time it rejoins the mesh and cannot retrieve a database from a GSS peer in the mesh. When the load is complete, the local database on the GSS device contains a full version of the sticky database.

If you want the local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, you can identify a favored GSS peer for that GSS device. By identifying a favored GSS peer, you can also reduce network issues with peer synchronization, which typically generate a burst of network traffic. In this case, direct network traffic to a peer other than the GSS identified as being the closest (with the shortest round-trip time).

When you identify a favored peer, the local GSS node, upon reentry into the mesh, always attempts to synchronize its sticky database entries with the favored GSS peer. If the GSS favored peer is unavailable, the local GSS node queries the remaining mesh peers to find the closest up-to-date sticky database.

Network connectivity issues, GSS devices leaving and rejoining the mesh, and GSS device restarts have a minor impact on the synchronization of the sticky database. Sticky database entries always reconverge based on their usage and the user-configurable sticky inactivity timeout values.

Logging in to the CLI and Enabling Privileged EXEC Mode



Note

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

DNS Sticky Quick Start Guide

Table 8-1 provides a quick overview of the steps required to configure the GSS for DNS sticky operation, both local and global DNS sticky. Each step includes the primary GSSM command required to complete the task. For the procedures to configure the GSS for DNS sticky, see the sections that follow the table.

Table 8-1 DNS Sticky Configuration Quick Start

Task and Command Example

1. If you are using global sticky with multiple GSS devices, log in to the CLI of each GSS in the mesh, enable privileged EXEC mode, and synchronize its system clock with an NTP server.

For example, enter:

```
gssm1.example.com> enable
gssm1.example.com# config
gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
gssm1.example.com(config)# ntp enable
```

2. Enter the global server load-balancing configuration mode.

For example, enter:

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

3. Use the **sticky-properties** command to enter the sticky properties configuration mode.

For example, enter:

```
gssm1.example.com(config-gslb)# sticky-propertie
gssm1.example.com(config-gslb-stkyprop)#
```

4. From the sticky properties configuration mode, enable sticky and specify a mode (global or local).

For example, to enable global DNS sticky for the GSS network, enter:

```
gssm1.example.com(config-gslb-stkyprop)# enable global
gssm1.example.com(config-gslb-stkyprop)# exit
gssm1.example.com(config-gslb)#
```

Table 8-1 DNS Sticky Configuration Quick Start (continued)**Task and Command Example**

5. Configure default DNS sticky configuration and inter-GSS global sticky mesh settings in sticky properties configuration mode. You can use the following keywords and arguments:
 - **encryption**—Enables or disables the encryption of data transmitted by GSS devices in the mesh. Valid options are as follows:
 - **enable**—Enables the encryption of data transferred between GSS peers in the mesh.
 - **key name**—Provides a secret string key for authentication between GSS devices as well as for encryption (if enabled).
 - **mask netmask**—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses as an attempt to increase the number of clients that the sticky database can support.
 - **timeout seconds**—Specifies the maximum time period that an unused answer remains valid in the sticky database.
 - **favored-peer**—If you want a local GSS device to attempt synchronization with a specific favored GSS peer upon reentry into the sticky mesh, specify a GSS device and a favored GSS peer (a different GSS device) combination for each local GSS device in the mesh.

See the “[Configuring DNS Sticky](#)” section for a complete description of these settings.

For example, enter:

```
gssm1.example.com(config-gslb-stkyprop)# enable global
gssm1.example.com(config-gslb-stkyprop)# encryption key SECRETKEY
gssm1.example.com(config-gslb-stkyprop)# timeout 120
gssm1.example.com(config-gslb-stkyprop)# exit
gssm1.example.com(config-gslb)#
```

6. Develop your DNS rule using the **dns rule** command.

For example, enter:

```
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# dns rule drule02 owner
WEB-SERVICES source-address-list WEB-GLOBAL-LISTS domain-list
E-COMMERCE query A
gssm1.example.com(config-gslb-rule[rule-name])#
```

Table 8-1 DNS Sticky Configuration Quick Start (continued)**Task and Command Example**

7. Define how the GSS supports DNS stickiness in a DNS rule (by domain or domain-list) by entering the **sticky method** command as follows:

```
gssm1.example.com(config-gslb-rule[rule-name])# sticky method
domain
gssm1.example.com(config-gslb-rule[rule-name])#
```

8. If you want to override the global timeout value set for the DNS rule, specify a new **timeout** value.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# sticky method
domain timeout 250
gssm1.example.com(config-gslb-rule[rule-name])#
```

9. Configure Balance Clause 1 for the DNS rule by entering the **clause** command and use the **sticky enable** option to enable sticky for the DNS rule.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1
vip-group ANSGRP-VIP-01 sticky enable
gssm1.example.com(config-gslb-rule[rule-name])#
```

Table 8-1 DNS Sticky Configuration Quick Start (continued)

Task and Command Example

10. (Optional) Configure other **clause** command settings as appropriate. You can use the following keywords and arguments:
- **count number**—Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule.
 - **ttl number**—Specifies the duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer.
 - **method**—(Optional) Specifies the method type for each balance clause. Method types are as follows:
 - **round-robin**—The GSS cycles through the list of answers that are available as requests are received. This is the default.
 - **ordered**—The GSS selects an answer from the list based on precedence.
 - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group.
 - **weighted-round-robin**—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.
 - **hashed**—The GSS selects the answer based on a unique value created from information stored in the request. Valid hashed method types are: **source-address**, **domain-name**, or **both**.

See the [“Adding Sticky to a DNS Rule that uses VIP-Type Answer Groups”](#) section for a complete description of these settings.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1  
vip-group ANSGRP-VIP-01 sticky enable ttl 30 method ordered  
gssm1.example.com(config-gslb-rule[rule-name])#
```

Table 8-1 DNS Sticky Configuration Quick Start (continued)**Task and Command Example**

11. Using the **clause** command, repeat Steps 9 and 10 for Balance Clause 2.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 2
vip-group ANSGRP-VIP-02 sticky enable ttl 60 method least-loaded
gssm1.example.com(config-gslb-rule[rule-name])#
```

Note The GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

12. Reenter the **clause** command for Balance Clause 3, and then repeat Steps 9 and 10.

13. (Optional) Group multiple D-proxy IP addresses as a single entry in the sticky database, exit from the rule configuration mode, and then use the **sticky group** command in global server load-balancing mode.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# exit
gssm1.example.com(config-gslb)# sticky group StickyGroup1 ip
192.168.3.0 netmask 255.255.255.0
```

Synchronizing the GSS System Clock with an NTP Server

If you are using global sticky in your GSS network, you must synchronize the clocks of all GSS devices in the mesh to enable a GSS to communicate with the other GSS devices in the peer mesh. If a GSS system clock is out of synchronization with the other GSS peers (by a value greater than 3 minutes), that GSS will ignore update messages from other GSS devices until you synchronize its system clock.

**Note**

We strongly recommend that you synchronize the system clock of each GSS in the mesh with a Network Time Protocol (NTP) server. NTP is a protocol designed to synchronize the clocks of computers over a network with a dedicated time server.

You must specify the NTP servers for each GSS device that operates in the global mesh before you enable DNS sticky for those devices from the primary GSSM. This sequence ensures that the clocks of each GSS device are synchronized before they join the global sticky peer mesh.

**Note**

For details on logging in to a GSS device and enabling privileged EXEC mode at the CLI, see the [“Logging in to the CLI and Enabling Privileged EXEC Mode”](#) section.

Use the **ntp-server** global configuration mode command to specify one or more NTP servers for GSS clock synchronization. The syntax for this CLI command is as follows:

```
ntp-server ip_or_host
```

The *ip_or_host* argument specifies the IP address or hostname of the NTP time server in your network that provides the clock synchronization. You can specify a maximum of four IP addresses or hostnames. Enter the IP address in dotted-decimal notation (for example, 172.16.1.2) or a mnemonic hostname (for example, myhost.mydomain.com).

Use the **ntp enable** global configuration mode command to enable the NTP service. The syntax of this CLI command is as follows:

```
ntp enable
```

This example shows how to specify the IP addresses of two NTP time servers for a GSS device and enable the NTP service:

```
gssm1.example.com> enable  
gssm1.example.com# config  
gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3  
gssm1.example.com(config)# ntp enable
```

Configuring Sticky Using the Primary GSSM CLI

This section describes how to configure GSS devices for DNS sticky operation, add stickiness to a DNS rule on the primary GSSM, and manage the sticky database. It contains the following topics:

- [Configuring DNS Sticky](#)
- [Enabling Sticky in a DNS Rule](#)
- [Creating Sticky Groups](#)
- [Deleting Entries from the Sticky Database](#)
- [Dumping Sticky Database Entries](#)
- [Running a Periodic Sticky Database Backup](#)
- [Loading Sticky Database Entries](#)

Configuring DNS Sticky

The GSS includes a set of DNS sticky settings that function as the default values used by the GSS network when you enable sticky in a DNS rule. You can configure sticky only in a DNS rule that uses a VIP-type answer group. In addition, sticky is active for a DNS rule only when the following conditions exist:

- Sticky is enabled for either global or local use. In the CLI, enter the **enable global** or **enable local** command.
- A sticky method option (domain or domain list) is selected. In the CLI, enter the **sticky method domain** or **sticky method domain list** command.
- Sticky is enabled within a balance clause for the DNS rule. In the CLI, enter the **sticky enable** command.

From global server load-balancing configuration mode, use the **sticky-properties** command to enter the sticky properties configuration mode. In the sticky properties configuration mode, you can enter commands to enable sticky and modify the DNS sticky settings for the GSS network. Sticky settings are applied as soon as you exit from the sticky properties configuration mode or enter a new mode.

To enable sticky and configure the sticky settings from the sticky properties configuration mode, specify one or more of the following commands:

- **enable**—Enables DNS sticky for the global or local level. Valid options are:
 - **global**—Enables global DNS sticky for each active GSS device across the entire GSS mesh. With global DNS sticky, all local sticky features are in operation and each GSS device in your network shares answers between peer GSS devices in a peer mesh. The peer mesh attempts to ensure that if any GSS device in the mesh receives the same question, then the same answer is returned to the requesting client D-proxy.
 - **local**—Enables DNS sticky for each active GSS device on a local level only. Each GSS attempts to ensure that subsequent requests for the same domain name are “stuck” to the same location as the first request. Sticky database information is not shared between GSS devices in the GSS mesh.
- **encryption**—Enables or disables the encryption of data transmitted by GSS devices in the mesh. This command is valid only if the **global** command is enabled. The GSS support encryption of all inter-GSS communications to maintain the integrity of the sticky database information transferred among the mesh peers. This command is disabled by default (data is transmitted in clear text). Valid options are as follows:
 - **enable**—Enables the encryption of data transferred between GSS peers in the mesh. Each GSS uses the Message Digest 5 (MD5)-based hashing method to encrypt the application data sent throughout the mesh.
 - **key name**—(Optional) Provides a secret string key for authentication between GSS devices as well as for encryption (if enabled). Enter a unique alphanumeric name with a maximum of 31 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **mask netmask**—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses in order to increase the number of clients that the sticky database can support. This mask is applied to the client source IP address before accessing the sticky database. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). The default global mask is 255.255.255.255.

When you define a DNS sticky group for incoming D-proxy addresses (see the “[Creating Sticky Groups](#)” section) and the incoming D-proxy address does not match any of the entries in a defined DNS sticky group, the GSS uses this global netmask value to calculate a grouped D-proxy network address.

- **timeout seconds**—Specifies the maximum time that an unused answer remains valid in the sticky database. This value defines the sticky database entry age-out process. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. Enter a value from 15 to 10080 minutes (168 hours), specified in 5 minute intervals (15, 20, 25, 30, and up to 10080). The default value is 60 minutes.

You can also individually set the **timeout** value for each DNS rule. When you set a **timeout** value for a DNS rule, that value overrides the global **timeout** value.


Note

The sticky timeout is accurate to within 5 minutes of the specified value. Each entry will persist in the sticky database for the configured sticky timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

- **favored-peer**—If you want a local GSS device to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, specify a favored peer for each local GSS device in the mesh. By specifying a favored GSS peer, you can also reduce network issues with peer synchronization, which typically generate a burst of network traffic. In this case, you can direct network traffic to a peer other than the GSS identified as being the closest (with the shortest round-trip time). This command is valid only if you enable the **global** option. Specify one of the following:
 - *GSS*—Name of the local GSS device that will be associated with a favored peer GSS device. The peer GSS device is the name of another GSS device that you specify in the *GSS-peer* variable.
 - *GSS-peer*—Name of the favored GSS peer that is to be associated with the GSS device name specified as the *GSS* variable.

Reenter the **favored-peer** command as many times as required to assign favored GSS peers to the GSS devices in the sticky mesh.

A GSS joins the mesh when any of the following occur:

- A reload.
- A power up.

- When you issue the **gss stop** and **gss start** command sequence.
- When you enter the **reload** command
- When you enter the **sticky stop** and **sticky start** command sequence
- When you enable the **global** option.

Upon reentry into the mesh, the local GSS device first attempts to synchronize its sticky database entries with its favored GSS peer. If the favored peer is unavailable, the GSS queries the remaining mesh peers to find the closest up-to-date sticky database (with the shortest round-trip time).

For example, assume there are four GSS devices in a mesh (gss_1, gss_2, gss_3, and gss_4), and both gss_1 and gss_2 are in the bootup process. You can direct local device gss_1 to gss_3 as its GSS peer, and direct local device gss_2 to gss_4 as its GSS peer. The identification of favored GSS peers in the mesh can prevent those GSS devices that are booting from waiting for another database request to complete before their database synchronization request can be serviced.

If you do not specify any favored GSS peers, the GSS uses the shortest round-trip time to prioritize which peers to request a database update.

- **mask netmask**—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses as an attempt to increase the number of clients that the sticky database can support. This mask is applied to the client source IP address before accessing the sticky database. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). The default global mask is 255.255.255.255.

When you define a DNS sticky group for incoming D-proxy addresses (see the “[Creating Sticky Groups](#)” section) and any incoming D-proxy address does not match any of the entries in a defined DNS sticky group, the GSS uses this global netmask value to calculate a grouped D-proxy network address.

- **timeout minutes**—Specifies the maximum time that an unused answer remains valid in the sticky database. This value defines the sticky database entry age-out process. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. Enter a value from 15 to 10080 minutes (168 hours), specified in 5-minute intervals (15, 20, 25, 30, and up to 10080). The default value is 60 minutes.

You can also individually set the **timeout** value for each DNS rule. When you set a **timeout** value for a DNS rule, that value overrides the global **timeout** value.



Note The sticky timeout is accurate to within 5 minutes of the specified value. Each entry will persist in the sticky database for the configured sticky timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

For example, to enable global stickiness and specify encryption key and timeout values, enter:

```
gssm1.example.com(config-gslb)# sticky-properties
gssm1.example.com(config-gslb-stkyprop)# enable global
gssm1.example.com(config-gslb-stkyprop)# encryption key SECRETKEY
gssm1.example.com(config-gslb-stkyprop)# timeout 120
gssm1.example.com(config-gslb-stkyprop)# exit
gssm1.example.com(config-gslb)#
```

To reset a stickiness setting to its default, use the **no** form of the command as follows:

```
gssm1.example.com(config-gslb-stkyprop)# no timeout 120
gssm1.example.com(config-gslb-stkyprop)# no mask 255.255.255.0
gssm1.example.com(config-gslb-stkyprop)# exit
gssm1.example.com(config-gslb)#
```

Enabling Sticky in a DNS Rule

This section contains the following topics:

- [Sticky DNS Rule Overview](#)
- [Adding Sticky to a DNS Rule that uses VIP-Type Answer Groups](#)

Sticky DNS Rule Overview

After you enable DNS sticky and configure sticky settings, you add stickiness to a DNS rule using the **sticky method** and **clause** commands in rule configuration mode. The GSS supports DNS stickiness in a DNS rule on either a matching domain (**domain** option) or on a matching domain list (**domain-list** option). The

domain and domain-list sticky methods instruct the GSS that all requests from a client D-proxy for a matching hosted domain or domain list are to be given the same answer for the duration of a user-configurable sticky time period.

Enabling sticky in a DNS rule clause causes the GSS to look up in the sticky database for a matched entry based on a combination of D-proxy IP address and requested domain information, and if the answer is found, to return the answer as the DNS response to the requesting D-proxy. If the answer is in the offline state, or the GSS does not find the answer, it evaluates the balance method clauses in the DNS rule to choose a new answer.

You can configure sticky individually for each balance clause in a DNS rule. However, the GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

**Note**

If you use DNS sticky and network proximity in your DNS rule, stickiness always takes precedence over proximity. When a valid sticky answer exists for a given DNS rule match, the GSS does not consider proximity when returning an answer to a client D-proxy.

Adding Sticky to a DNS Rule that uses VIP-Type Answer Groups

To add sticky to a DNS rule that uses VIP-type answer groups, perform the following steps:

1. If you have not already done so, enable local or global DNS sticky. See the [“Configuring DNS Sticky”](#) section for details.
2. Develop your DNS rule by using the **dns rule** command, as described in the [“Building DNS Rules”](#) section of [Chapter 7, Building and Modifying DNS Rules](#).
3. Define how the GSS supports DNS stickiness in a DNS rule by using the **sticky method** command with one of the following options:

- **domain**—Enables DNS stickiness on a domain. For all requests from a single D-proxy, the GSS sends the same answer for a domain. For rules matching on a domain wildcard (for example, *.cisco.com), entries are stuck together using the global configuration ID assigned to the wildcard. The GSS does not attempt to distinguish the individual domains that match the wildcard.
- **domain-list**—Enables DNS stickiness on a matching domain list. The GSS groups all domains in the domain list and treats them as a single hosted domain. The GSS treats wildcards in domain lists the same as non-wildcard domains.

**Note**

Sticky is disabled by default. When disabled, the GSS answers DNS requests for all domains and clients that pertain to the DNS rule, subject to DNS rule matching, without accessing the sticky database or sharing sticky database information between peers in the network.

4. Override the global timeout value set for a DNS rule by specifying a new **timeout** value. Enter the maximum time interval that can pass without the sticky database receiving a lookup request for an entry. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. Enter a value from 15 to 10080 minutes, defined in 5-minute intervals (15, 20, 25, 30, and up to 10080).

For example, enter:

```
gssm1.example.com(config-gslb)# dns rule drule02
gssm1.example.com(config-gslb-rule[rule-name])# sticky method
domain timeout 250
gssm1.example.com(config-gslb-rule[rule-name])#
```

**Note**

The sticky **timeout** is accurate to within 5 minutes of the specified value. Each entry will persist in the sticky database for the configured sticky timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

5. Configure Balance Clause 1 using the **clause** *number* **vip-group** *name* command in the rule configuration mode. The syntax for this command is as follows:

```
clause number vip-group name [count number | sticky {enable | disable} | ttl number | method {round-robin | least-loaded | ordered | weighted-round-robin | hashed {domain-name | source-address | both}}]
```

The keywords and arguments for this command are as follows:

- **number**—Balance Clause 1, 2, or 3. You can specify a maximum of three balance clauses that use VIP-type answers.
- **vip-group** *name*—Specifies the name of a previously created VIP-type answer group.
- **count** *number*—(Optional) Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule. The default is 1 record.
- **sticky**—(Optional) Specify **enable** to activate sticky for the clause. Specify **disable** (the default) to deactivate sticky for the clause. To specify **enable**, make sure that the **sticky method** option (see Step 3) is set to **domain** or **domain-list**.
- **ttl** *number*—(Optional) Specifies the time-to-live duration in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer. Valid entries are 0 to 604,800 seconds. The default is 20 seconds.
- **method**—(Optional) Specifies the method type for each of your balance clauses. Method types are as follows:
 - **round-robin**—The GSS cycles through the list of answers that are available as requests are received. This is the default.
 - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request. The least-loaded option is available only for VIP-type answer groups that use a KAL-AP keepalive.
 - **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports numbering gaps in an ordered list.

**Note**

For answers that have the same order number in an answer group, the GSS will use only the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

—weighted-round-robin—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.

—hashed—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group. Enter one of the following:

- **domain-name**—The GSS selects the answer based on a hash value created from the requested domain name.
- **source-address**—The GSS selects the answer based on a hash value created from the source address of the request.
- **both**—The GSS selects the answer based on both source-address and domain name.

6. Repeat the configuration process for Balance Clauses 2 and 3 by entering the **clause** command.

**Note**

The GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction also applies if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

For example, to set up Balance Clauses 1 and 2 with stickiness for the previously created DNS rule named drule02, enter:

```
gssm1.example.com(config-gslb)# dns rule drule02
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group
ANSGRP-VIP-01 sticky enable method ordered
gssm1.example.com(config-gslb-rule[rule-name])# clause 2 vip-group
ANSGRP-VIP-02 sticky enable method least-loaded
gssm1.example.com(config-gslb-rule[rule-name])#
```

To delete a balance clause, use the **no** form of the **clause** command as follows:

```
gssm1.example.com(config-gslb-rule[rule-name])# no clause 2 vip-group
ANSGRP-VIP-02 sticky enable method least-loaded
gssm1.example.com(config-gslb-rule[rule-name])#
```

Creating Sticky Groups

The primary GSSM supports the creation of sticky groups. A sticky group allows you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its sticky database as a single entry. Instead of multiple sticky database entries, the GSS uses only one entry in the sticky database for multiple D-proxies. The GSS treats all D-proxies in a sticky group as a single D-proxy.

This section contains the following topics:

- [DNS Sticky Group Overview](#)
- [Creating a DNS Sticky Group](#)
- [Deleting a Sticky Group IP Address Block](#)
- [Deleting a Sticky Group](#)

DNS Sticky Group Overview

Create sticky groups from the primary GSSM CLI to obtain better scalability of your configuration and to allow easy sticky group creation through automated scripts. The primary GSSM supports a maximum of 800 sticky groups. Each sticky group contains one to 30 blocks of IP addresses and subnet masks (in dotted-decimal notation).

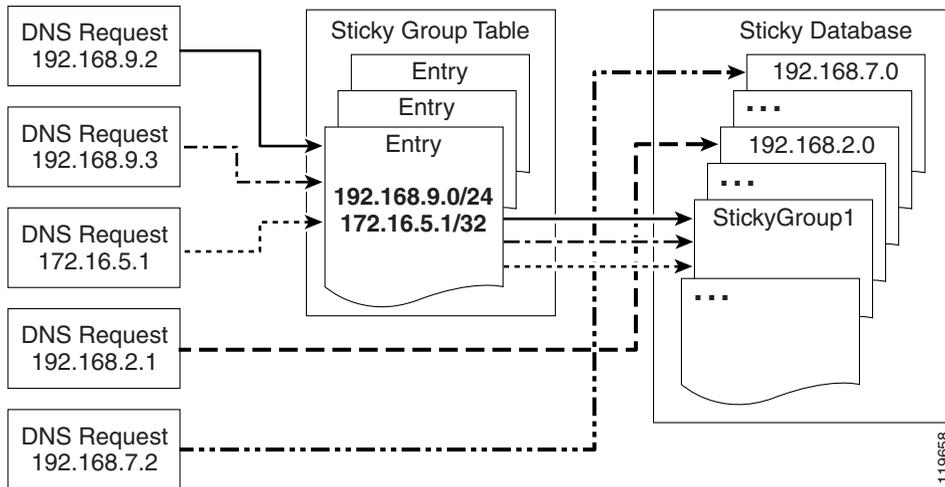
Grouping D-proxy IP addresses in the sticky database allows you to address proxy hopping. Certain ISPs rotate their D-proxies. A user's browser may use DNS server A to resolve a hostname and later use DNS server B to resolve the same name. This technique is referred to as proxy hopping because the DNS sticky function remembers the client's D-proxy IP address and not the IP address of the actual client. Thus, rotating D-proxies appear to the GSS as unique clients. Sticky grouping allows you to globally group sets of D-proxies to solve this proxy hopping problem.

In addition to creating DNS sticky groups of multiple D-proxy IP addresses from the CLI, you can configure a global netmask to uniformly group contiguous D-proxies (see the [“Configuring DNS Sticky”](#) section). The global netmask is

used by the GSS device when no DNS sticky group matches the incoming D-proxy address. The GSS uses the full incoming D-proxy IP address (255.255.255.255) and the global netmask as the key to look up in the DNS sticky database. The default global mask is 255.255.255.255.

Figure 8-1 shows how through DNS sticky group entries 192.168.9.0 255.255.255.0 and 172.16.5.1 255.255.255.255, the DNS requests from D-proxies 192.168.9.2, 192.168.9.3, and 172.16.5.1 all map to the identified group name, *StickyGroup1*. If no match is found in the sticky group table for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 8-1 Locating a Grouped Sticky Database Entry



Creating a DNS Sticky Group

You can create a DNS sticky group by using the **sticky group** global server load-balancing command from the primary GSSM CLI to identify the name of the DNS sticky group and add an IP address block to the group. Use the **no** form of the command to delete a previously configured IP address block from a sticky group or to delete a sticky group.

At the CLI of the primary GSSM, you create sticky groups to obtain better scalability of your configuration and to allow easy sticky group creation through automated scripts. The sticky groups are saved in the primary GSSM database and all GSS devices in the network receive the same sticky group configuration. You cannot create sticky groups using the CLI of a standby GSSM or individual GSS devices.

The syntax for this command is as follows:

```
sticky group groupname ip ip-address netmask netmask
```

The options and variables are as follows:

- *groupname*—A unique alphanumeric name for the DNS sticky group; Use a maximum of 80 characters and avoid names that include spaces since they are not allowed.
- **ip** *ip-address*—Specifies the IP address block in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmask*—Specifies the subnet mask of the IP address block in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to create a sticky group called *StickyGroup1* with an IP address block of 192.168.9.0 255.255.255.0:

```
gssm1.example.com# config  
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# sticky group StickyGroup1 ip  
192.168.9.0 netmask 255.255.255.0
```

Reenter the **sticky group** command if you want to perform one of the following tasks:

- Add multiple IP address blocks to a DNS sticky group
- Create additional DNS sticky groups

Each sticky group can have a maximum of 30 blocks of defined IP addresses and subnet masks. The GSS prohibits duplication of IP addresses and subnet masks among DNS sticky groups.

Deleting a Sticky Group IP Address Block

You can delete a previously configured IP address block from a sticky group by using the **no** form of the **sticky group ip** command as follows:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no sticky group StickyGroup1 ip
192.168.3.0 netmask 255.255.255.0
```

Deleting a Sticky Group

You can delete a sticky group by using the **no** form of the **sticky group** command as follows:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no sticky group StickyGroup1
```

Deleting Entries from the Sticky Database

You can remove entries from the sticky database of each GSS device by using the **sticky database delete** command. When operating in a global sticky configuration, the result of the **sticky database delete** command propagates throughout the GSS mesh to maintain synchronization between the peers in the GSS network.



Caution

Use the **sticky database delete all** command when you want to remove all entries and empty the sticky database. Ensure that you want to permanently delete entries from the sticky database before you enter this command since you cannot retrieve sticky database entries once you delete them.

To view the entries in the sticky database to identify the sticky entries that you want to delete, use the **show sticky database** command (see the “[Displaying the Sticky Database Status](#)” section in [Chapter 13, Displaying GSS Global Server Load-Balancing Statistics](#)).

Use the **sticky database delete** command to remove entries from the sticky database. The syntax for this command is as follows:

```
sticky database delete {all | answer {name/ip_address} | domain {name} |  
domain-list {name} | group {name} | inactive minimum {minutes} |  
maximum {minutes} | ip {ip_address} | netmask {netmask} | rule  
{rule_name}}
```

The options and variables are as follows:

- **all**—Removes all entries from the sticky database memory. The prompt “Are you sure?” appears to confirm the deletion of all database entries. Specify **y** to delete all entries or **n** to cancel the deletion operation.
- **answer** *name/ip_address*—Removes all sticky entries related to a particular answer. Specify the name of the answer. If there is no name for the answer, specify the IP address of the sticky answer in dotted-decimal notation (for example, 192.168.9.0).
- **domain** *name*—Removes all sticky entries related to a domain. Specify the exact name of a previously created domain.
- **domain-list** *name*—Removes all sticky entries related to a domain list. Specify the exact name of a previously created domain list.
- **group** *name*—Removes all sticky entries related to a sticky group. Specify the exact name of a previously created sticky group.
- **inactive minimum** *minutes* **maximum** *minutes*—Removes all sticky entries that have not received a lookup request by a client D-proxy in the specified minimum and maximum time interval. Valid entries are 0 to 10100 minutes. If you do not specify a maximum value, the GSS deletes all entries that have been inactive for the specified minimum value or longer. The GSS returns an error if one of the following situations occur:
 - The maximum value is set to a value that is less than the minimum value.
 - The minimum and maximum values are not within the allowable range of values for the sticky inactivity timeout.

- **ip** *ip_address netmask netmask*—Removes all sticky entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **rule** *rulename*—Removes all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

For example, to remove the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gssm1.example.com# sticky database delete ip 192.168.8.0 netmask  
255.255.255.0
```

Dumping Sticky Database Entries

The GSS automatically dumps sticky database entries to a backup file on disk approximately every 20 minutes. The GSS uses this backup file to initialize the sticky database upon system restart or reboot to enable the GSS to recover the contents of the database. When global sticky is enabled, the GSS restores from the database dump file any time it reenters the mesh and cannot retrieve the sticky database contents from a GSS peer in the mesh.

You can dump all entries or selected entries from the sticky database to a named file as a user-initiated backup file. You can then use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the file to and from remote machines.

To view the entire contents of a sticky database XML output file from the GSS, use the **type** command. See the *Cisco Global Site Selector Administration Guide* for details about displaying the contents of a file.

The GSS includes options that provide a level of granularity for dumping entries from the sticky database. The GSS supports binary and XML output formats. Optionally, you can specify the entry type filter to clarify the information dumped from the sticky database.

If you specify a format but do not specify an entry type, the GSS automatically dumps all entries from the sticky database.

If you attempt to overwrite an existing sticky database dump file with the same filename, the GSS displays the following message:

```
Sticky Database dump failed, a file with that name already exists.
```

Use the **sticky database dump** command to output entries from the sticky database. The syntax for this command is as follows:

```
sticky database dump {filename} format {binary | xml} entry-type {all | group | ip}
```

The options and variables are as follows:

- **filename**—Name of the output file that contains the sticky database entries on the GSS disk. This file resides in the /home directory.
- **format**—Dumps the sticky database entries in a binary or XML format. Choose the binary encoding as the format type if you intend to load the contents of the file into the sticky database of another GSS. The valid entries are as follows:
 - **binary**—Dumps the assigned sticky entries in true binary format. This file can be used only with the **sticky database load** command.
 - **xml**—Dumps the assigned sticky entries in an XML format. The contents of an XML file includes the data fields and the data descriptions. The contents of this file can be viewed using the **type** command. See [Appendix B, “Sticky and Proximity XML Schema Files”](#) for information on defining how content appears in output XML files.



Note Dumping sticky database entries in an XML format can be a resource intensive operation and may take from 2 to 4 minutes to complete depending on the size of the sticky database and the GSS platform in use. We recommend that you do not perform a sticky database dump in an XML format during the routine operation of the GSS to avoid a degradation in performance.

- **entry-type**—Specifies the type of sticky database entries to dump. The valid entries are as follows:
 - **all**—Dumps all entries from the sticky database
 - **group**—Dumps all entries that have sticky group IDs from the database
 - **ip**—Dumps all entries that have source IP addresses from the database

This example shows how to dump the D-proxy source IP addresses from the sticky database to the sdb2004_06_30 file in XML format. For large numbers of entries, progress messages may appear.

```
gssm1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Starting Sticky Database dump.

gssm1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump is in progress...
Sticky Database has dumped 15678 of 34512 entries

gssm1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump completed. The number of dumped entries: 34512
gssm1.example.com#
```

When the dump finishes, a “completed” message displays and the CLI prompt reappears.

Running a Periodic Sticky Database Backup

You can instruct the GSS to dump sticky database entries to an output file on the GSS disk before the scheduled time. You may want to initiate a sticky database dump as a database recovery method to ensure that you store the latest sticky database entries before you shut down the GSS.

To force an immediate backup of the sticky database residing in GSS memory, use the **sticky database periodic-backup now** command. The GSS sends the sticky database entries to the system dump file as the sticky database file. Upon a reboot or restart, the GSS reads this file and loads the contents to initialize the sticky database at boot time.

The syntax for this command is as follows:

```
sticky database periodic-backup now
```

For example, enter:

```
gssm1.example.com# sticky database periodic-backup now
```

Loading Sticky Database Entries

The GSS supports the loading and merging of sticky database entries from a file into the existing sticky database in GSS memory. The merge capability supports the addition of entries from one GSS to another GSS. The file must be in binary format for loading into GSS memory.

The GSS validates the loaded database entries, checks the software version for compatibility, and then adds the sticky database entries in memory. The GSS does not overwrite duplicate entries in the sticky database.

Use the **sticky database load** command to load and merge a sticky database from disk into the existing sticky database in GSS memory. The syntax for this command is as follows:

```
sticky database load filename
```



Note

If you want to load and replace all sticky database entries from a GSS instead of merging the entries with the existing sticky database, enter the **sticky database delete all** command to remove all entries from sticky database memory before you enter the **sticky database load** command.

Specify the name of the sticky database file to load and merge with the existing sticky database on the GSS device. The file must be in binary format for loading into GSS memory (see the [“Dumping Sticky Database Entries”](#) section). Use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the sticky database file to the GSS from a remote GSS.

This example shows how to load and merge the entries from the GSS3SDB file with the existing entries in the GSS sticky database:

```
gssm1.example.com# sticky database load GSS3SDB
```

Disabling DNS Sticky Locally on a GSS for Troubleshooting

You can disable DNS sticky for a single GSS when you need to locally override the globally-enabled sticky option to troubleshoot or debug the device. The GSS does not store the local-disable setting in its running-configuration file. When you restart the device and sticky has been enabled from the primary GSSM, the GSS reenables DNS sticky.

Use the **sticky stop** and **sticky start** commands to locally override the sticky enable option of the primary GSSM.

When you enter the **sticky stop** command, the GSS immediately stops the following operations:

- Sticky lookups in the sticky database
- Accessing the sticky database for new requests
- Periodic sticky database dumps
- Sticky database entry age-out process

The GSS continues to answer DNS requests according to the DNS rules and keepalive status.

When you locally disable sticky on a GSS, sticky remains disabled until you perform one of the following actions:

- Enter the **sticky start** CLI command.
- Enter the **gss restart** CLI command to restart the GSS software.
- Enter the **reload** CLI command to perform a cold restart of the GSS device.

If you are using global DNS sticky in your network, upon reentry of the GSS device into the peer mesh, the GSS attempts to synchronize the database entries with the other peers in the mesh. The GSS queries each peer to find the closest up-to-date sticky database. If no update is available from a peer, the GSS initializes the sticky database entries from the previously saved database on the disk if a file is present and valid. Otherwise, the GSS starts with an empty sticky database.

This example shows how to use the **sticky stop** command to locally disable DNS sticky on a GSS device:

```
gssm1.example.com# sticky stop
```

This example shows how to use the **sticky start** command to locally reenable DNS on the GSS device:

```
gssm1.example.com# sticky start
```




Configuring Network Proximity

This chapter describes how to configure a GSS to perform network proximity to determine the best (most proximate) resource for handling global load-balancing requests.

This chapter contains the following major sections:

- [Network Proximity Overview](#)
- [Proximity Network Design Guidelines](#)
- [Network Proximity Quick Start Guide](#)
- [Configuring a Cisco Router as a DRP Agent](#)
- [Synchronizing the GSS System Clock with an NTP Server](#)
- [Creating Zones Using the Primary GSSM CLI](#)
- [Configuring Proximity Using the Primary GSSM CLI](#)
- [Initiating Probing for a D-proxy Address](#)
- [Disabling Proximity Locally on a GSS for Troubleshooting](#)
- [Where to Go Next](#)

Each GSS supports a comprehensive set of **show** CLI commands to display network proximity statistics for the device. In addition, the primary GSSM GUI displays statistics about proximity operation for the GSS network. See [Chapter 13, Displaying GSS Global Server Load-Balancing Statistics](#), for details about viewing network proximity statistics.

Network Proximity Overview

The GSS responds to DNS requests with the most proximate answers (resources) relative to the requesting D-proxy. Proximity refers to the distance or delay in terms of network topology, not geographical distance, between the requesting client's D-proxy and its answer.

To determine the most proximate answer, the GSS communicates with a probing device, a Cisco IOS-based router, located in each proximity zone to gather round-trip time (RTT) metric information measured between the requesting client's D-proxy and the zone. Each GSS directs client requests to an available server with the lowest RTT value.

The proximity selection process is initiated as part of the DNS rule balance method clause. When a request matches the DNS rule and balance clause with proximity enabled, the GSS responds with the most proximate answer.

This section describes the major functions in GSS network proximity:

- [Proximity Zones](#)
- [Probe Management and Probing](#)
- [Proximity Database](#)
- [Example of Network Proximity](#)

Proximity Zones

A network can be logically partitioned into zones based on the arrangement of devices and network partitioned characteristics. A zone can be geographically related to data centers in a continent, a country, or a major city. All devices, such as web servers in a data center, that are located in the same zone have the same proximity value when communicating with other areas of the Internet.

You can configure a GSS proximity network with a maximum of 32 zones. Within each zone, there is an active probing device that is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one probing device to a requesting D-proxy.

A location is a method to logically group devices in data centers for administrative purposes. A location can represent a physical point, such as a building or a rack. When you use the GSS to perform network proximity, each location must be assigned to a zone. In addition, you assign each answer used in a GSS proximity DNS rule to a location that is associated with a zone. This configuration hierarchy informs the GSS about resources when determining the most proximate answer.

Probe Management and Probing

Probe management is the intelligence behind each GSS device's interaction with the probing device in a zone. Within each zone, there must be at least one probing device and, optionally, a backup probing device. If the primary probing device fails, the probes are redirected to the backup device. Once the primary probing device becomes available, probes are redirected back to the primary probing device.

The GSS uses Director Response Protocol (DRP) to communicate with the probing devices (called DRP agents) in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems. You can use any Cisco router as the probing device in a zone that can support the DRP agent software and measure ICMP, TCP, or path-probe RTT. The GSS communicates with the Cisco IOS-based router using the DRP RTT query and response method.

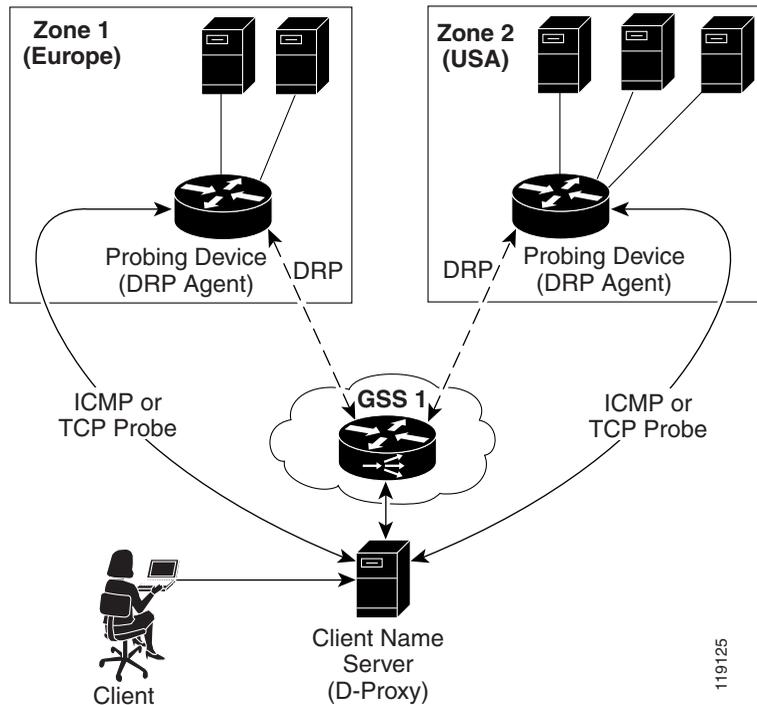
Each DRP agent accepts probing instructions from the GSS and returns probing results to the GSS based on the DRP protocol. DRP allows for the authentication of packets exchanged between the DRP agent and the GSS.

The GSS transmits DRP queries to one or more probing devices in the GSS network, instructing the DRP agent in the probing device to probe specific D-proxy IP addresses. Each probing device responds to the query by using a standard protocol, such as ICMP or TCP, to measure the RTT between the DRP agent in the zone and the IP address of the requesting client's D-proxy device.

When the GSS receives a request from a D-proxy, it decides if it can provide a proximate answer. If the GSS is unable to determine a proximate answer from the proximity database (PDB), it sends a probe to one or more probing devices to get proximity information between those probing devices and the new D-proxy. After the GSS receives the probing results, it adds the RTT information to the PDB.

Figure 9-1 shows the probing process between a GSS (DRP client) and a probing device (DRP agent).

Figure 9-1 *DRP Communication in a GSS Network*



The GSS supports two type of probing methods:

- **Direct Probing**—Direct probing occurs between the GSS and DRP agents when the GSS creates a dynamic entry in the PDB as the result of receiving a new D-proxy IP address. Direct probing also occurs when you specify alternative IP addresses as targets for the probing devices to obtain RTT data and add static entries in the PDB. The GSS initiates direct probing to the DRP agent when a request is made for a new D-proxy IP address entry. Through direct probing, the GSS automatically sends probe requests to the DRP agent in each zone to obtain initial probe information as quickly and efficiently as possible for the new entries in the PDB.

- Refresh Probing—The GSS periodically reprobes the actively used D-proxies to obtain the most up-to-date RTT values and store these values in the PDB. The RTT values reflect recent network changes. The refresh probe interval is a user-configured selection.

**Note**

Static entries in the PDB created with static RTT values do not use direct or refresh probing. The configured static RTT is always returned during proximity lookup regardless of the configured acceptable available percentage of zones.

Proximity Database

The PDB provides the core intelligence for all proximity-based decisions made by a GSS. Proximity lookup occurs when a DNS rule is matched and the associated clause has the proximity option enabled. When the GSS receives a request from a D-proxy and decides that a proximity response should be provided, the GSS identifies the most proximate answer (the answer with the smallest RTT time) from the PDB that resides in GSS memory and sends that answer to the requesting D-proxy. If the PDB is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from probing devices in every zone in the proximity network, and puts the results in the PDB.

For example, a GSS communicates with three zones to determine the most proximate answer and receives the following RTT values from the probing devices in each zone to a particular client D-proxy:

- Zone1 = 100 ms
- Zone2 = 120 ms
- Zone3 = 150 ms

From the three RTT values in the PDB, the GSS selects Zone1 as the most proximate zone for the client's D-proxy request because it has the smallest RTT value.

The GSS supports a maximum of 500,000 D-proxy IP address entries in the PDB table, including both dynamic and static entries. The GSS creates dynamic entries in the PDB as the result of requests for new D-proxy IP addresses. If necessary, you can add static entries to the PDB by specifying permanent RTT values (gathered by other means), and optionally, alternative IP addresses to probe.

The primary GSSM supports the creation of proximity groups that allow you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its PDB as a single entry. Instead of multiple PDB entries, the GSS uses only one entry in the PDB for multiple D-proxies. The GSS treats all D-proxies in a proximity group as a single D-proxy when responding to DNS requests with the most proximate answers. Requests from D-proxies within the same proximity group receive the RTT values from the database entry for the group. The benefits of proximity grouping are as follows:

- Fewer probing activities performed by the GSS
- Less space required for the PDB
- Greater user flexibility in assigning alternative probing targets or static proximity metrics to a group

The dynamic entries in the PDB age out based on the user-specified global inactivity setting to keep the PDB size manageable. The inactivity timeout setting defines the maximum period of time that can occur without a PDB entry receiving a lookup request, after which the GSS deletes the entry from the PDB.

When the total number of entries in the PDB exceeds 480,000, the GSS automatically removes the least recently used entries. The GSS determines the least recently used entries as those dynamic entries in the PDB that have not been hit within a fixed cutoff time of 60 minutes (one hour). The GSS does not automatically remove static entries from the PDB. You must manually delete PDB static entries from the GSS CLI.

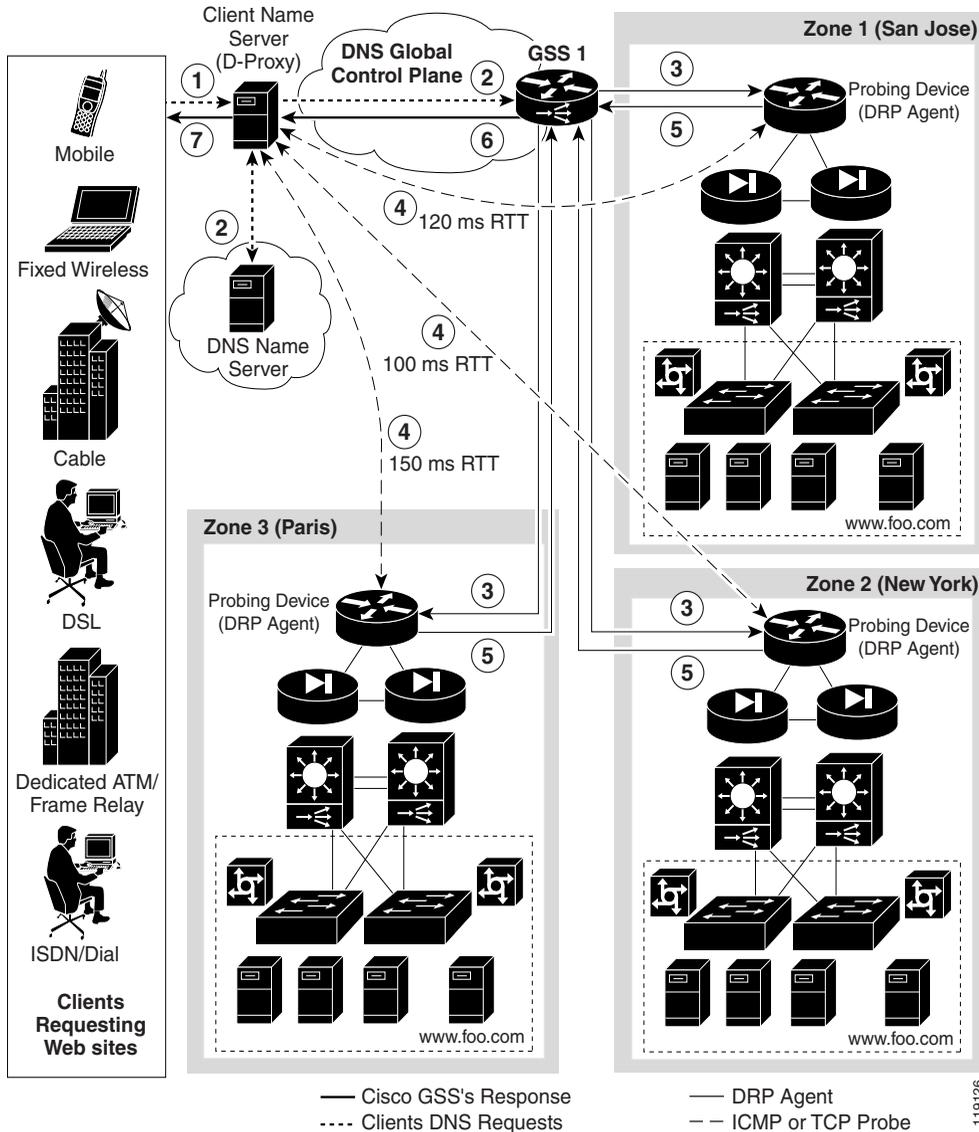
When the PDB reaches a maximum of 500,000 entries, the GSS does not add entries to the PDB and any new requests for answers result in a failure. The GSS tracks how many entries are dropped when the maximum limit has been reached. Once the number of PDB entries drops below 500,000, the GSS resumes adding new entries to the PDB.

Example of Network Proximity

The process outlined below describes how the GSS interacts with the probing devices in multiple zones to perform network proximity. See [Figure 9-2](#) for an illustration of the following steps.

1. A client performs an HTTP request for `www.foo.com`. The content for this website is supported at three different data centers.
2. The DNS global control plane infrastructure processes this request and directs the client D-proxy to GSS 1. The GSS offloads the site selection process from the DNS global control plane. The client's local D-proxy queries GSS1 for the IP address associated with `www.foo.com`. The GSS accepts the DNS query.
3. If the request matches a proximity DNS rule configured on the GSS, the GSS performs an internal PDB lookup. If the lookup fails, the GSS sends DRP queries to the DRP agent configured for each zone.
4. When the DRP agent in each zone receives a DRP request, it measures the RTT from the associated zone back to the requesting client D-proxy device, using either ICMP, TCP, or a path-probe.
5. After calculating DRP RTT metrics, the DRP agents send their replies to the GSS. The GSS sorts the DRP RTT replies from the DRP agents to identify the best (smallest) RTT metric. The DRP agent then returns the smallest RTT metric that identifies the closest zone, which in [Figure 9-2](#) is Zone 2 (New York).
6. The GSS returns to the client's local D-proxy one or more IP address records (DNS A resource records) that match the DNS rule and correspond to the best or most proximate server (`www.foo.com`) located in Zone 2 (New York).
7. The client's local D-proxy returns the IP address that corresponds to `www.foo.com` to the client that originated the request. The client transparently connects to the server in Zone 2 for `www.foo.com`.

Figure 9-2 Network Proximity Using the Cisco Global Site Selector



Proximity Network Design Guidelines

When developing your proximity network, ensure that you include a sufficient number of GSS devices to support the expected load. Follow these guidelines when designing your proximity network:

- Decide how many zones you require for your proximity network based on your current network configuration and the level of proximity that you require for your network. A maximum of 32 zones is allowed within each GSS proximity environment. You can change the zone configuration at any time by deleting or adding a zone, or by moving a zone from one location to another location.
- For each zone, identify the probing device and optionally the back up the probing device. Each probing device represents the topological location of its associated zone and also reflects the zone's expected network behavior in terms of connectivity to the Internet. The probing device is the DRP agent located within the zone.
- Each GSS network can contain a maximum of eight GSS devices. You can add or delete GSS devices at any time. The GSS does not have to reside within a zone.
- To use proximity, you must do the following:
 - Associate a proximity zone with a location.
 - Assign a location that is associated with a proximity zone to an answer.

To use an answer group with a proximity balance method, the answers in the answer group must be contained in locations that are tied to a zone.

Network Proximity Quick Start Guide

Table 9-1 provides a quick overview of the steps required to configure the GSS for proximity network operation. Each step includes the primary GSSM CLI command required to complete the task. For the procedures to configure the GSS for proximity, see the sections that follow the table.

Table 9-1 Proximity Configuration Quick Start

Task and Command Example

1. Log in to the CLI of each GSS in the network, enable privileged EXEC mode, and synchronize its system clock with an NTP server.

For example, enter:

```
gssm1.example.com> enable
gssm1.example.com# config
gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
gssm1.example.com(config)# ntp enable
```

2. Configure a Cisco router as a DRP agent in one or more proximity zones.
3. Enter the global server load-balancing configuration mode.

For example, enter:

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

4. Configure a proximity zone from the primary GSSM by entering the **zone** command.

For example, enter:

```
gssm1.example.com(config-gslb)# zone Z1 index 1 probe
192.168.11.1 backup probe 192.168.11.5
```

5. Access the proximity properties configuration mode by entering the **proximity-properties** command in global server load-balancing configuration mode.

For example, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)#
```

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

6. From the proximity properties configuration mode, enable proximity.

For example, enter:

```
gssm1.example.com(config-gslb-proxprop)# enable  
gssm1.example.com(config-gslb-proxprop)# exit  
gssm1.example.com(config-gslb)#
```

7. Configure global proximity configuration default settings using the following commands in proximity properties configuration mode:
- **mask** *netmask*—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of supported D-proxies in the PDB. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
 - **timeout** *minutes*—Specifies the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry.
 - **equivalence** *number*—Specifies a percentage value that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Use this command to adjust the granularity of the proximity decision process.
 - **refresh-interval** *hours*—Specifies the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB.
 - **discovery-sequence**—Specifies the type of probe method (TCP, ICMP, or path-probe) used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically chooses a different probe method to contact the D-proxy.
 - **acceptable-rtt** *number*—Specifies a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. Use this command to adjust the granularity of the proximity decision process.

Table 9-1 Proximity Configuration Quick Start (continued)**Task and Command Example**

- **acceptable-zone** *number*—Specifies a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The value specifies the percentage of all zones configured and used for a DNS rule and answer group.
- **wait enable**—Enables the GSS proximity wait-state.
- **authentication drp enable**—Enables the DRP authentication state.
- **key drp**—If you enabled **authentication drp enable** and no DRP keys exist for the GSS, use this command to create a DRP authentication key. Repeat the command to make additional keys. Each DRP key includes a key identification number and a key authentication string.

See the “[Configuring Proximity](#)” section for a complete description of these settings.

For example, to enable global proximity and specify settings, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# enable
gssm1.example.com(config-gslb-proxprop)# mask 255.255.255.255
gssm1.example.com(config-gslb-proxprop)# timeout 4320
gssm1.example.com(config-gslb-proxprop)# equivalence 20
gssm1.example.com(config-gslb-proxprop)# refresh-interval 6
gssm1.example.com(config-gslb-proxprop)# discovery-sequence icmp
gssm1.example.com(config-gslb-proxprop)# acceptable-rtt 100
gssm1.example.com(config-gslb-proxprop)# acceptable-zone 40
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

8. (Optional) Enable DRP authentication and create a DRP key by entering the **authentication drp enable** and **key drp** commands.

For example, to create two new DRP keys, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# enable
gssm1.example.com(config-gslb-proxprop)# key drp 10 DRPKEY1
gssm1.example.com(config-gslb-proxprop)# key drp 20 DRPKEY2
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

9. (Optional) Associate a location to a proximity zone by using the **location** command in global server load-balancing configuration mode. Repeat this step for each location that you want to assign to a proximity zone.

For example, to associate the zone **z3** with the location **London**, enter:

```
gssm1.example.com(config-gslb)# location London zone z3  
gssm1.example.com(config-gslb)#
```

10. (Optional) Assign a location associated with a proximity zone to an answer by using the **answer vip ip_address** command in global server load-balancing configuration mode. Repeat this step for each answer that you want to assign to an associated proximity location.

For example, to associate the location "Paris" with the VIP answer called "SEC-PARIS2" enter:

```
gssm1.example.com(config-gslb)# answer vip 172.16.27.6 name  
SEC-PARIS2 location Paris  
gssm1.example.com(config-ansvip[ans-ip])
```

11. Develop your DNS rule by using the **dns rule** command.

For example, enter:

```
gssm1.example.com(config)# gslb  
gssm1.example.com(config-gslb)# dns rule drule03 owner  
WEB-SERVICES source-address-list WEB-GLOBAL-LISTS domain-list  
E-COMMERCE query A  
gssm1.example.com(config-gslb-rule[rule-name])#
```

12. Configure Balance Clause 1 for the DNS rule by using the **clause** command and the **proximity enable** option to enable proximity for the DNS rule.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1  
vip-group method ordered ANSGRP-VIP-03 proximity enable  
gssm1.example.com(config-gslb-rule[rule-name])#
```

Table 9-1 Proximity Configuration Quick Start (continued)**Task and Command Example**

13. (Optional) Modify other **clause** command settings for proximity as appropriate. See the [“Adding Proximity to a DNS Rule that uses VIP-Type Answer Groups”](#) section for a complete description of all settings available for the **clause** command. You can modify the following proximity settings:
- **rtt number**—Changes the proximity-acceptable RTT for the balance clause to a different value from the global proximity configuration.
 - **wait enable/disable** —Changes the proximity wait state to a different setting than the global proximity configuration.
 - **zone number**—Changes the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration.

For example, to set up Balance Clause 1 with proximity for a previously created DNS rule, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 1
vip-group ANSGRP-VIP-03 method ordered proximity enable rtt 75
zone 50
```

14. Using the **clause** command again, repeat Steps 12 and 13 for Balance Clause 2.

For example, enter:

```
gssm1.example.com(config-gslb-rule[rule-name])# clause 2
vip-group ANSGRP-VIP-03 method ordered proximity enable rtt 120
zone 55
gssm1.example.com(config-gslb-rule[rule-name])#
```

15. Reenter the **clause** command for Balance Clause 3, and then repeat Steps 12 and 13.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

16. (Optional) Group multiple D-proxy IP addresses as a single entry in the PDB to reduce probing and to take up less space, access the global server load-balancing configuration mode, and create a proximity group at the primary GSSM. Do so by using the **proximity group** command to add multiple D-proxy IP addresses and subnet masks to the group.

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip
192.168.3.0 netmask 255.255.255.0
```

17. (Optional) Add static proximity entries to the PDB of a GSS device in your network, access the global server load-balancing configuration mode, and use the **proximity assign** command to create static entries.

For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP2
zone-data "1:100,2:200,3:300,4:400,5:500"
```

Configuring a Cisco Router as a DRP Agent

When you enable DRP on a Cisco router, the router gains the additional functionality of operating as a DRP agent in the GSS network. A DRP agent can communicate with multiple GSSs and support multiple distributed servers.

This section includes the following background information about choosing and configuring the Cisco router in each proximity zone as a DRP agent. It contains the following topics:

- [Choosing a Cisco Router as a DRP Agent](#)
- [Configuring the DRP Agent](#)
- [Cisco IOS Release 12.1 Interoperability Considerations](#)

Choosing a Cisco Router as a DRP Agent

When selecting a Cisco router as the DRP agent in a zone, ensure that the:

- DRP agent is topologically close to each distributed server that it supports in the zone.
- DRP agent in the Cisco IOS-based router is configured to perform ICMP or TCP echo-based RTT probing.

Configuring the DRP Agent

You can configure and maintain the DRP agent in the Cisco IOS-based router by performing the tasks described in the “Configuring a DRP Server Agent” section, of the *Cisco IOS IP Configuration Guide*. The Cisco IOS-based router must support the DRP protocol in a proximity zone. DRP is supported in the following Cisco IOS Release trains: 12.1, 12.1E, 12.2T, 12.2, 12.3, and later releases. ICMP probing is supported only in Cisco IOS Release 12.2T, 12.3, and later.

The GSS operates with Cisco IOS-based routers using the following DRP RTT probing methods: TCP (“DRP Server Agent”) and ICMP (“ICMP ECHO-based RTT probing by DRP agents”). The Cisco IOS feature names shown in the Cisco Feature Navigator II are: “DRP Server Agent” and “ICMP ECHO-based RTT probing by DRP agents.”

The following process is required to configure a Cisco IOS-based router as a DRP agent:

1. Enable the DRP agent in the Cisco router.
2. Enable security for DRP by defining a standard access list that permits requests from only the GSS device. As a security measure, limit the source of valid DRP queries. If a standard IP access list is applied to the interface, the DRP agent responds only to DRP queries that originate from an IP address in the list. If no access list is configured, the DRP agent answers all queries.
3. Ensure that the router accepts DRP queries from the IP addresses associated with only the standard access list.
4. If necessary, set up Message Digest (MD5) authentication with passwords as another security measure. Enable the DRP authentication key chain, define the key chain, identify the keys associated with the key chain, and specify how long each key is to be valid. If MD5 authentication is configured on a

DRP agent, the GSS device must be similarly configured to recognize messages from that MD5 authentication-configured DRP agent and any other DRP agents configured for MD5 authentication.

Cisco IOS Release 12.1 Interoperability Considerations

If you use a GSS in a network proximity zone configuration with a router running Cisco IOS Release 12.1, you should ensure the DRP authentication configuration is identical on both devices. For example, if you intend to perform DRP authentication between a GSS and a router running Release 12.1, ensure that you properly enable and configure authentication on both devices. The same is true if you choose not to use DRP authentication; you must disable authentication on both devices.

If you disable DRP authentication on a router running Cisco IOS Release 12.1 but enable DRP authentication on a GSS, all measurement probes sent by a GSS to the router will fail. This occurs because the router fails to recognize the DRP echo query packets sent by a GSS and the GSS cannot detect a potential failure of measurement packets sent to the router. The GSS identifies the router as being ONLINE in its **show statistics proximity probes detailed** CLI command, yet the measurement response packets monitored in the Measure Rx field do not increment. These two conditions may indicate a DRP authentication mismatch.

If the DRP probe requests fail between the GSS and a Cisco router running Release 12.1, even if the GSS indicates that the router is ONLINE, verify the DRP authentication configurations on both the GSS and the Cisco router as follows:

- For the Cisco router running IOS Release 12.1, enter the **show ip drp** command. If the line “Authentication is enabled, using "test" key-chain” appears in the output (where “test” is the name of your key-chain), DRP authentication is configured on the router. If this line does not appear in the output, DRP authentication is not configured.
- For the Primary GSSM, enter the **show gslb-config proximity-properties** command to view the state of the authentication drp enable setting (see the “[Configuring Proximity](#)” section for details).

Modify the DRP authentication configuration on either the router running Cisco IOS Release 12.1 or the primary GSSM and make them consistent to avoid a DRP authentication mismatch.

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Synchronizing the GSS System Clock with an NTP Server

We strongly recommend that you synchronize the system clock of each GSS device in your network with a Network Time Protocol (NTP) server. NTP is a protocol designed to synchronize the clocks of computers over a network with a dedicated time server.

Synchronizing the system clock of each GSS ensures that the PDB and probing mechanisms function properly by having the GSS internal system clock remain constant and accurate within the network. Changes in the GSS system clock can affect the time stamp used by PDB entries and the probing mechanism used in a GSS.

You must specify the NTP server(s) for each GSS device operating in the proximity network before you enable proximity for those devices from the primary GSSM. This sequence ensures that the clocks of each GSS device are synchronized.

**Note**

For details on logging in to a GSS device and enabling privileged EXEC mode at the CLI, see the [“Creating Proximity Groups”](#) section.

Use the **ntp-server** global configuration mode command to specify one or more NTP servers for GSS clock synchronization. The syntax for this CLI command is as follows:

```
ntp-server ip_or_host
```

The *ip_or_host* argument specifies the IP address or hostname of the NTP time server in your network that provides the clock synchronization. You can specify a maximum of four IP addresses or hostnames. Enter the IP address in dotted-decimal notation (for example, 172.16.1.2) or a mnemonic hostname (for example, myhost.mydomain.com).

Use the **ntp enable** global configuration mode command to enable the NTP service. The syntax of this CLI command is as follows:

```
ntp enable
```

This example shows how to specify the IP addresses of two NTP time servers for a GSS device and enable the NTP service:

```
gssm1.example.com> enable  
gssm1.example.com# config  
gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3  
gssm1.example.com(config)# ntp enable
```

Creating Zones Using the Primary GSSM CLI

A proximity zone is a logical grouping of network devices that also contains one active probing device and a possible backup probing device. A zone can be geographically related to a continent, a country, or a major city. Each zone can include one or more locations. A location is a method to logically group collocated devices for administrative purposes.

During the proximity selection process, the GSS chooses the most proximate zones that contain one or more valid answers based on RTT data received from the probing devices configured in the zone. You can configure a proximity network with a maximum of 32 zones.

This section includes the following procedures:

- [Configuring a Proximity Zone](#)
- [Deleting a Proximity Zone](#)
- [Associating a Proximity Zone With a Location](#)
- [Associating a Proximity-Based Location with an Answer](#)

Configuring a Proximity Zone

To configure a proximity zone from the primary GSSM, use the **zone** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
zone name {index number | probe ip_address} [backup probe ip_address]
```

The options for this command are as follows:

- **name**—Zone name. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **index number**—Specifies the numerical identifier of the proximity zone. Enter an integer from 1 to 32. There is no default.
- **probe ip_address**— Specifies the IP address of the primary probe device that services this zone. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

- **backup probe** *ip_address*—(Optional) Specifies the IP address of a backup probe device that services this zone. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

For example, enter:

```
gssm1.example.com(config-gslb)# zone Z1 index 1 probe 192.168.11.1
backup 192.168.11.5
```

To modify the properties for a previously created zone, enter:

```
gssm1.example.com(config-gslb)# zone Z1 index 1 probe 192.168.11.2
backup 192.168.11.9
```



Note You cannot modify the **index** value. To change the zone index, delete the zone (see the [“Deleting a Proximity Zone”](#) section), and then create a new zone containing a different index.

Deleting a Proximity Zone

Use the **no** form of the **zone** command to delete a zone.

For example, to delete zone “z1,” enter:

```
gssm1.example.com(config-gslb)# no zone Z1 index 1 probe 192.168.11.1
backup 192.168.11.5
```

OR

```
gssm1.example.com(config-gslb)# no zone Z1
```

Associating a Proximity Zone With a Location

You can associate an existing proximity zone with a location by using the **location** command in global server load-balancing configuration mode. You can make the association for a new location or for an existing location. To display a list of existing locations, use the **show gslb-config location** command. See the [“Displaying Resource Information”](#) section in [Chapter 2, Configuring Network Proximity](#), for more information.

The syntax for the **location** command is as follows:

```
location name [region name | comments text | zone name]
```

The keywords and arguments for this command are as follows:

- **location** *name*—Geographical group name entities such as a city, data center, or content site for the location. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **region** *name*—(Optional) Specifies a region with which the location will be associated. There should be a logical connection between the region and location. Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **comments** *text*—(Optional) Specifies descriptive information or important notes about the location. Enter up to 256 alphanumeric characters. Comments with spaces must be entered in quotes.
- **zone** *name*—(Optional) Specifies the name of an existing zone that is to be associated with the location. There should be a logical connection between the zone and the location.

For example, to create a location named San_Francisco and associate it with the region Western_USA and the zone z1, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# location SAN_FRANCISCO region
WESTERN_USA zone z1
```

To associate the zone "z3" with the location London, enter:

```
gssm1.example.com(config-gslb)# show gslb-config location
...
location London region Western_EU
...
gssm1.example.com(config-gslb)# location London zone z3
gssm1.example.com(config-gslb)#
```

Associating a Proximity-Based Location with an Answer

You can assign a location that is associated with a proximity zone to an answer by using the **answer vip** *ip_address* command in global server load-balancing configuration mode. You can make the association for a new answer or for an existing answer. To display a list of existing answers, use the **show gslb-config answer** command. See the “[Displaying Answer Properties](#)” section in [Chapter 6, Configuring Answers and Answer Groups](#), for more information.

The syntax of the **answer vip** command is as follows:

```
answer vip ip_address [name name | location name | active | suspend]
```

The keywords and arguments for this command are as follows:

- *ip_address*—Specifies the VIP address field to which the GSS will forward requests. Enter an unquoted text string in <A.B.C.D> format.
- **name** *name*—(Optional) Specifies a name for the VIP-type answer that you are creating. Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **location** *name*—(Optional) Specifies an existing location name with which the answer is to be associated. See the “[Configuring Owners](#)” section in [Chapter 2, Configuring Network Proximity](#).
- **active**—(Optional) Reactivates a suspended VIP answer. This is the default.
- **suspend**—(Optional) Suspends an active VIP answer.

For example, to create a VIP answer called "SEC-LONDON1" and associate it with the "London" location, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# answer vip 10.86.209.232 name
SEC-LONDON1 location LONDON
gssm1.example.com(config-ansvip[ans-ip])
```

To associate the location Paris with the VIP answer called SEC-PARIS2 enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer
...
answer vip 172.16.27.6 name SEC-PARIS2 active
      keepalive type tcp port 180 active
...
```

```
gssm1.example.com(config-gslb)# answer vip 172.16.27.6 name SEC-PARIS2  
location Paris  
gssm1.example.com(config-ansvip[ans-ip])
```

Configuring Proximity Using the Primary GSSM CLI

This section describes how to configure the GSS for network proximity from the primary GSSM CLI, how to add proximity to a DNS rule, and how to manage the proximity database. It contains the following topics:

- [Configuring Proximity](#)
- [Creating DRP Keys](#)
- [Deleting DRP Keys](#)
- [Adding a Proximity Balance Clause to a DNS Rule](#)
- [Creating Proximity Groups](#)
- [Configuring Static Proximity Database Entries](#)
- [Deleting Entries from the Proximity Database](#)
- [Dumping Proximity Database Entries to a File](#)
- [Running a Periodic Proximity Database Backup](#)
- [Loading Proximity Database Entries](#)

Configuring Proximity

The GSS contains proximity settings that function as the default values used by the GSS network when you enable proximity in a DNS rule.

From global server load-balancing configuration mode, use the **proximity-properties** command to enter the proximity properties configuration mode. In the proximity properties configuration mode, enable proximity and modify the DNS proximity settings for the GSS network. Proximity settings are applied as soon as you exit from the proximity properties configuration mode or enter a new mode.

To enable proximity and configure the proximity settings from the proximity properties configuration mode, specify one or more of the following commands:

- **enable**—Enables global proximity across the entire GSS network. This command is disabled by default.
- **mask *netmask***—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses as an attempt to increase the number of supported D-proxies in the PDB. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). The default global mask is 255.255.255.255.

When you define a proximity group for incoming D-proxy addresses, and an incoming D-proxy address does not match any of the entries in a defined proximity group, the GSS uses this global netmask value to calculate a grouped D-proxy network address. See the “[Creating Proximity Groups](#)” section for more information.

- **timeout *minutes***—Specifies the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry. This value defines the PDB entry age-out process. Once an entry reaches the inactivity time, the GSS removes the selected dynamic entries from the PDB. Enter a value from 5 to 10080 minutes (168 hours). The default value is 4320 minutes (72 hours).
- **equivalence *number***—Specifies a percentage that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Through the equivalence percentage, you define an RTT window that the GSS uses to consider zones equal. The equivalence value enables the GSS to prioritize between multiple distributed servers that have similar server-to-client RTT values. The GSS considers any RTT value that is less than or equal to the lowest RTT plus the percentage to be equivalent to the lowest RTT value. The GSS chooses one answer from a set of answers in equal zones.

For example, with an equivalence setting of 20 percent and a series of returned RTT values:

- Zone1 = RTT of 100 ms
- Zone2 = RTT of 120 ms
- Zone3 = RTT of 150 ms

The GSS determines that Zone1 has the lowest RTT value. In this case, the GSS adds 20 percent (20 ms) to the RTT value to make Zone1 and Zone2 equally proximate in regards to the GSS selecting an answer. The RTT equivalence window range is 100 ms to 120 ms, and the GSS considers any zone that returns an RTT value in that range to be equally proximate.

Use this parameter to adjust the granularity of the proximity decision process. Enter an equivalence value from 0 to 100 percent. The default value is 20 percent.

- **refresh-interval** *hours*—Specifies the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. Enter a value from 1 to 72 hours. The default value is 8 hours.
- **discovery-sequence**—Specifies the type of probe method used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically chooses a different probe method to contact the D-proxy. The available choices for the initial probe method are as follows:
 - **tcp**—The probing device uses the TCP SYN-ACK and RST handshake sequence to probe the user-specified TCP port and measure the RTT between the probing device and the D-proxy. You can configure the source and destination TCP ports on the router.
 - **icmp**—The probing device uses an ICMP echo request and response to measure the RTT between the probing device and the D-proxy.
- **path-probe**—This is a fallback method for ICMP/TCP probes and cannot be selected as the initial probe method. It is only supported on the GSS acting as a DRP agent and by default, is not enabled.

When the GSS fails to receive the minimum acceptable RTT metrics from the DRP agents, it sends a query message to the probing devices configured for each zone instructing the DRP agent running on the GSS to probe using the path-probe method instead. If at least one of the DRP agents returns RTT using the legacy ICMP/TCP probing methods, the path-probe is not triggered.

**Note**

The path-probe technique makes a best effort to calculate the relative RTT for those D-proxies behind the firewall. This method involves tracing the path along with the RTT to all intermediate gateways between the probing device and the D-proxy. The calculated path information is then sent back to the querying GSS.

The metrics obtained from the DRP agents configured for each zone are compared by the GSS to arrive at a common gateway. The best (smallest) RTT metric to the first common gateway is used to determine the closest content serving site. This method differs from the ICMP/TCP probe method by calculating RTT to the common gateway, not to the D-proxy.

- **acceptable-rtt number**—Specifies a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. If the zones configured on the GSS report an RTT that is less than the specified acceptable-rtt value, the GSS does the following:
 - a. Disregards the acceptable percentage of zones.
 - b. Considers that there is sufficient proximity data to make a proximity decision.
 - c. Uses the zones reporting less than or equal to this value in the proximity decision.

Use this setting to adjust the granularity of the proximity decision process. Enter an acceptable-rtt value from 50 to 1500 ms. The default value is 100 ms.

- **acceptable-zone number**—Specifies a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The value specifies the percentage of all zones configured and used for a DNS rule and answer group. If an insufficient number of zones report RTT information, the balance clause fails and the GSS processes a new clause. For example, if the answer group associated with a clause includes answers that correspond to 5 different zones and you specify an acceptable-zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of 2 zones to satisfy the 40-percent criteria. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

Use this parameter to adjust the granularity of the proximity decision process. Enter a percentage of zones from 3 to 100 percent. The default value is 40 percent.



Note If the reported RTT from one or more zones for the DNS rule/answer group is below the acceptable-rtt value, then the acceptable-zone value is ignored by the GSS.

- **wait enable/disable**—Instructs the GSS to wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process. In the disabled state (the default), the GSS does not wait to perform a proximity selection if it has not received the appropriate RTT and zone information based on other proximity settings. Instead, the GSS proceeds to the next balance clause in the DNS rule.
- **authentication drp enable**—Instructs the GSS to authenticate packets that it exchanges with the DRP agent in a probing device through the exchange of DRP keys (see the **key drp** command). The key authenticates the DRP requests and responses sent between the GSS and the DRP agent. In the disabled state (the default), the GSS does not perform DRP authentication with the DRP agent. See the [“Creating DRP Keys”](#) section for more information.
- **key drp**—If you enabled the **authentication drp enable** command (see above), create one or more DRP keys. Each DRP key contains a key identification number and a key authentication string. The primary GSSM supports a maximum of 32 keys.

Specify the following settings for the **key drp** command:

- *id_number*—The identification number of a secret key used for encryption. The GSS uses the ID value to retrieve the key string that is used to verify the DRP authentication field. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS. You can add a maximum of 32 keys. The range of key identification numbers is 0 to 255.
- *auth_string*—The authentication string that is sent and received in the DRP packets. The string must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The string can contain 1 to 80 uppercase and lowercase alphanumeric characters. However, the first character cannot be a number.

See the [“Creating DRP Keys”](#) section for more information.

For example, to enable global proximity and specify settings, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# enable
gssm1.example.com(config-gslb-proxprop)# mask 255.255.255.0
gssm1.example.com(config-gslb-proxprop)# timeout 4320
gssm1.example.com(config-gslb-proxprop)# equivalence 20
gssm1.example.com(config-gslb-proxprop)# refresh-interval 6
gssm1.example.com(config-gslb-proxprop)# discovery-sequence icmp
gssm1.example.com(config-gslb-proxprop)# acceptable-rtt 100
gssm1.example.com(config-gslb-proxprop)# acceptable-zone 40
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

To reset various global proximity settings back to the default setting, use the **no** form of the command. For example, enter:

```
gssm1.example.com(config-gslb-proxprop)# no mask 255.255.255.0
gssm1.example.com(config-gslb-proxprop)# no timeout 4320
gssm1.example.com(config-gslb-proxprop)# no equivalence 20
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Creating DRP Keys

DRP supports the authentication of packets exchanged between the DRP agent (probing device) and the DRP client (the GSS). Use the **authentication drp enable** and **key drp** commands in proximity properties configuration mode to enable DRP authentication and create one or more DRP keys. See the [“Configuring Proximity”](#) section for details on these two commands. Each DRP key contains a key identification number and a key authentication string. The primary GSSM supports a maximum of 32 keys.

The DRP key is stored locally on each GSS in the network. The key functions as an encrypted password to help prevent DRP-based denial-of-service attacks, which can be a security threat. Each GSS generates DRP packets that contain all of the configured keys and sends the packets to the DRP agent in each configured zone. The DRP agent in each probing device examines the packet for a matching key (see the [“Configuring the DRP Agent”](#) section). If it finds a matching key, the DRP agent considers the DRP connection as authentic and accepts the packet.

For example, to create three new DRP keys, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# authentication drp enable
```

```
gssm1.example.com(config-gslb-proxprop)# key drp 10 DRPKEY1
gssm1.example.com(config-gslb-proxprop)# key drp 20 DRPKEY2
gssm1.example.com(config-gslb-proxprop)# key drp 30 DRPKEY3
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Deleting DRP Keys

You can remove DRP authentication keys by using the **no** form of the **key drp** command.

For example, enter:

```
gssm1.example.com(config-gslb-proxprop)# no key drp 30 DRPKEY3
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Adding a Proximity Balance Clause to a DNS Rule

This section contains the following topics:

- [Proximity Balance Clause Overview](#)
- [Adding Proximity to a DNS Rule that uses VIP-Type Answer Groups](#)

Proximity Balance Clause Overview

After you enable and configure network proximity from the primary GSSM, add proximity to a DNS rule for VIP-type answer groups using the **clause** command in rule configuration mode. The balance method configured in the matched clause of the DNS rule determines the answer that the GSS selects when multiple valid answers are present in the most proximate zones and returns this answer as the DNS response to the requesting D-proxy. If the GSS does not find an answer, it evaluates the other balance methods in the DNS rule to choose a new answer.

The GSS supports proximity in a DNS rule with the following balance methods:

- Ordered
- Round-robin
- Weighted-round-robin
- Least-loaded

You can configure proximity individually for the three balance clauses in a DNS rule. Proximity lookup occurs when the DNS rule is matched and the associated clause has the proximity option enabled. When the GSS receives a request from a D-proxy and decides that a proximity response should be provided, the GSS identifies the most proximate answer (the answer with the smallest RTT time) from the PDB residing in GSS memory and sends that answer to the requesting D-proxy. If the PDB is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from probing devices in every zone in the proximity network, and puts the results in the PDB.

When there are no valid answers in the answer group of a proximity balance clause, the GSS skips that balance clause and moves on to the next clause listed in the DNS rule unless you specify a proximity wait condition. In that case, the GSS waits to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process.

**Note**

If you use DNS sticky and network proximity in your DNS rule, stickiness always takes precedence over proximity. When a valid sticky answer exists for a given DNS rule match, the GSS does not consider proximity when returning an answer to a client D-proxy.

Adding Proximity to a DNS Rule that uses VIP-Type Answer Groups

To add proximity balance clauses to a DNS rule that uses VIP-type answer groups, perform the following steps:

1. If you have not already done so, configure and enable the global proximity settings. See the [“Configuring Proximity”](#) section for details.
2. Develop your DNS rule by using the **dns rule** command, as described in the [“Building DNS Rules”](#) section of [Chapter 7, Building and Modifying DNS Rules](#).
3. Configure Balance Clause 1 by using the **clause number vip-group name** command in the rule configuration mode.

The syntax for this command is as follows:

clause *number* **vip-group** *name* [**method** { **round-robin** | **least-loaded** | **ordered** | **weighted-round-robin** | **hashed** { **domain-name** | **source-address** | **both** } } | **count** *number* | **proximity** { **enable** [**rtt** *number* | **wait** { **enable** | **disable** } } | **zone** *number*] | **disable** } | **ttl** *number*]

The keywords and arguments for this command are as follows:

- **number**—Balance Clause number (1, 2, or 3). You can specify a maximum of three balance clauses that use VIP-type answers.
- **vip-group name**—Specifies the name of a previously created VIP-type answer group.



Note

Ensure that the answers in the answer group that you specify are contained in locations that are tied to a zone.

- **method**—(Optional) Specifies the method type for each balance clause. Method types are as follows:
 - **round-robin**—The GSS cycles through the list of answers that are available as requests are received. This is the default.
 - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request.

The least-loaded option is available only for VIP-type answer groups that use a KAL-AP keepalive.

- **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports numbering gaps in an ordered list.



Note

For answers that have the same order number in an answer group, the GSS will only use the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

–weighted-round-robin—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.

–hashed—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group. Enter one of the following:

- **domain-name**—The GSS selects the answer based on a hash value created from the requested domain name.
- **source-address**—The GSS selects the answer based on a hash value created from the source address of the request.
- **both**—The GSS selects the answer based on both the source address and domain name.
- **count number**—(Optional) Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule. The default is 1 record.
- **proximity**—(Optional) Specify **enable** or **disable**:

–enable—Activates proximity for the clause. When you specify **enable**, the following options are available:

- **rtt number**—Changes the proximity-acceptable RTT for the balance clause to value that differs from the global proximity configuration. The GSS uses this value as the user-specified acceptable RTT when determining the most proximate answer. See the **acceptable-rtt number** option in the [“Configuring Proximity”](#) section for details. Enter an acceptable RTT value from 50 to 1500 ms. The default value is 100 ms.
- **wait enable/disable**—Changes the proximity wait state to a setting that differs from the global proximity configuration. When enabled, the GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. When disabled, the GSS proceeds to the next balance clause in the DNS rule. See the **wait** option in the [“Configuring Proximity”](#) section for details.

- **zone number**—Changes the proximity-acceptable zone percentage for the balance clause to a value that differs from the global proximity configuration. This option specifies the percentage of all zones configured and is used for a DNS rule and answer group. See the **acceptable-zone** option in the “[Configuring Proximity](#)” section for details.
 - **-disable**—Deactivates proximity for the clause.
 - **tth number**—(Optional) Specifies the duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer. Valid entries are 0 to 604,800 seconds. The default is 20 seconds.
4. Repeat the configuration process for Balance Clauses 2 and 3 by using the **clause** command.

For example, to set up Balance Clauses 1 and 2 with proximity for the previously created DNS rule named `drule03`, enter:

```
gssm1.example.com(config-gslb)# dns rule drule03
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group
ANSGRP-VIP-03 method ordered proximity enable rtt 75 zone 50
gssm1.example.com(config-gslb-rule[rule-name])# clause 2 vip-group
ANSGRP-VIP-03 method least-loaded proximity enable rtt 125 zone 50
gssm1.example.com(config-gslb-rule[rule-name])#
```

Creating Proximity Groups

This section includes the following topics:

- [Proximity Group Overview](#)
- [Creating a Proximity Group](#)
- [Playing Static Proximity Group Configurations](#)
- [Deleting a Proximity Group IP Address Block](#)
- [Deleting a Proximity Group](#)

Proximity Group Overview

The primary GSSM supports the creation of proximity groups. A proximity group allows you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its PDB as a single entry. Instead of multiple PDB entries, the GSS uses only one entry in the PDB for multiple D-proxies. The GSS treats all D-proxies in a proximity group as a single D-proxy when responding to DNS requests with the most proximate answers. Requests from D-proxies within the same proximity group receive the RTT values from the database entry for the group.

You create proximity groups from the primary GSSM CLI to obtain better scalability of your configuration and to allow for easy proximity group creation through automated scripts. The primary GSSM supports a maximum of 5000 proximity groups. Each proximity group contains 1 to 30 blocks of IP addresses and subnet masks (in dotted-decimal format).

The benefits of proximity grouping include:

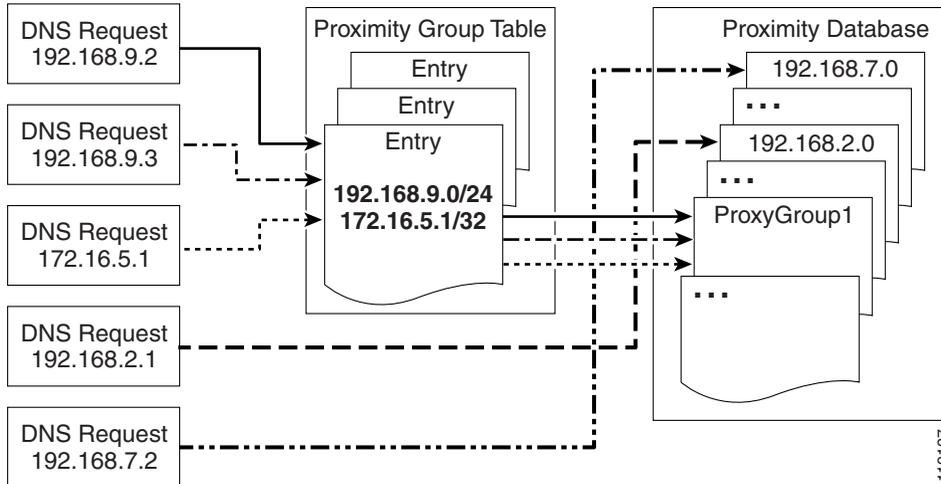
- Fewer probing activities performed by the GSS which reduces the overhead associated with probing. The GSS probes the first requesting D-proxy from all configured zones to obtain the RTT value from each zone for the entire proximity group.
- Less space required for the PDB. Instead of multiple PDB entries, the GSS uses only one entry for multiple D-proxies.
- Greater flexibility in assigning alternative probing targets or static proximity metrics to a group.

In addition to creating proximity groups of multiple D-proxy IP addresses from the CLI, you can configure a global netmask from the primary GSSM to uniformly group contiguous D-proxies (see the “[Configuring Proximity](#)” section). The global netmask is used by the GSS device when no proximity group matches the incoming D-proxy address. The GSS uses the full incoming D-proxy IP address (255.255.255.255) and the global netmask as the key to look up the proximity database. The default global mask is 255.255.255.255.

[Figure 9-3](#) shows how the DNS requests from D-proxies 192.168.9.2, 192.168.9.3, and 172.16.5.1 all map to the identified group name, ProxyGroup1, through proximity group entries 192.168.9.0/24 and 172.16.5.1/32. If no match is found in the PDB for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key.

In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 9-3 Locating a Grouped Proximity Database Entry



Creating a Proximity Group

From the primary GSSM CLI, you can create a proximity group by using the **proximity group** global server load-balancing configuration mode command to identify the name of the proximity group and add an IP address block to the group. Use the **no** form of the command to delete a previously configured IP address block from a proximity group or to delete a proximity group.

Create proximity groups at the CLI of the primary GSSM to obtain better scalability of your configuration and to allow easy proximity group creation through automated scripts. Proximity groups are saved in the primary GSSM database. All GSS devices in the network receive the same proximity group configuration. You cannot create proximity groups at the CLI of a standby GSSM or individual GSS devices.

The syntax for this command is as follows:

```
proximity group {groupname} ip {ip-address} netmask {netmask}
```

The options and variables are as follows:

- *groupname*—Unique alphanumeric name. Names must have a maximum of 80 characters and spaces are not allowed.
- **ip** *ip-address*—Specifies the IP address block in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmask*—Specifies the subnet mask of the IP address block in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to create a proximity group called ProxyGroup1 with an IP address block of 192.168.9.0 255.255.255.0:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip
192.168.9.0 netmask 255.255.255.0
```

Reenter the **proximity group** command if you want to perform the following:

- Add multiple IP address blocks to a proximity group
- Create additional proximity groups

Each proximity group can have a maximum of 30 blocks of defined IP addresses and subnet masks. The GSS prohibits duplication of IP addresses and subnet masks among proximity groups.

Playing Static Proximity Group Configurations

If the size of static proximity group configuration is quite large, you should use the **proximity play-config** command to play the static proximity configuration. This command plays the proximity commands more efficiently than **script play-config**.



Note

This command is only supported on the primary and secondary GSSM.

The syntax for this command is as follows:

```
proximity play-config filename
```

The *filename* specifies the file containing the proximity configuration.

To use this command, perform the following steps:

1. Ensure that the primary and secondary GSSMs are synchronized.
2. Stop the primary GSSM by entering the **gss stop** command.
3. Enter **proximity play-config** in privileged EXEC mode.
4. Bookmark the key that is generated after you enter the command.
5. Stop the secondary GSSM by entering the **gss stop** command.
6. Enter **proximity play-config** in privileged EXEC mode.
7. Enter the key generated from the primary GSSM at the prompt.



Note

You should ensure that the secondary GSSM is registered to the primary before entering **proximity play-config** on the primary GSSM.

This example shows how to play a static proximity configuration:

```
gssm1.example.com# proximity play-config prox.txt
Tue Mar 6 13:10:43 2007 waiting for postmaster to start...done
Tue Mar 6 13:10:43 2007 postmaster successfully started
proximity group proxal ip 11.1.1.4 netmask 255.255.255.252
proximity group proxal ip 11.1.1.8 netmask 255.255.255.252
.
.
.
proximity group proxa50 ip 11.1.2.140 netmask 255.255.255.252
proximity group proxa50 ip 11.1.2.144 netmask 255.255.255.252
#####
Please use the following Key required while, playing "proximity
play-config" on SGSSM.
Key: 8912515fa7339c1b60a20b60142493328b997b
#####
```

Deleting a Proximity Group IP Address Block

You can delete a previously configured IP address block from a proximity group by using the **no** form of the **proximity group** command. For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no proximity group ProxyGroup1 IP
192.168.9.0 netmask 255.255.255.0
```

Deleting a Proximity Group

You can delete a proximity group and all configured IP address blocks by using the **no** form of the **proximity group** command. For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gs1b
gssm1.example.com(config-gs1b)# no proximity group ProxyGroup1
```

Configuring Static Proximity Database Entries

This section describes how to configure static entries in the PDB. It contains the following topics:

- [Adding Static Proximity Entries](#)
- [Deleting Static Entries from the Proximity Database](#)

Adding Static Proximity Entries

In the PDB, entries can be both dynamic and static. The GSS creates dynamic entries in the PDB as the result of requests from new D-proxy IP addresses. If you need to configure static proximity metrics for zones in your GSS network or assign probing devices to specific D-proxies, you must define a series of static entries in the PDB by using the **proximity assign** global server load-balancing configuration mode command. If the same entry, dynamic or static, already exists in the proximity database, the GSS will overwrite that entry with the newly-assigned entry. You can use automated scripts if you intend to add numerous static entries in the PDB of each GSS.



Note

The **proximity assign** command affects only the local GSS. If you want to add the same static entries in the PDB of the other GSS devices in your network, enter the **proximity assign** command at CLI of each GSS.

Static entries in the PDB do not age out; they remain in the PDB until you delete them. Static entries are not subject to the automatic database cleanup of least recently used entries when the PDB size is almost at the maximum number of entries. Use the **no proximity assign** command to delete static entries from the PDB.

You can specify permanent RTT values for the static entries. When the GSS uses permanent RTT values, it does not perform active probing with the DRP agent. Instead of RTT values, you can specify alternative IP addresses as targets for probing by the probing devices to obtain RTT data. The GSS probes the alternative probe target for requests from D-proxies matching these static entries.

Static entries in the PDB are either static RTT-filled or probe-target IP-filled.

To create static entries in the PDB, use the **proximity assign** global server load-balancing configuration mode command. The syntax for this command is as follows:

```
proximity assign { group { groupname } } | ip { entryaddress } | [probe-target
{ ip-address } | zone-data { "zoneId:RTT" } ]
```


Note

The GSS accepts commands up to 1024 characters. Ensure that the **proximity assign** command does not exceed that length when you configure RTT for a large number of proximity zones.

The options and variable are as follows:

- **group** *groupname*—Specifies a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, "name 1"). Each static proximity group must have a unique name.
- **ip** *entryaddress*—Specifies the D-proxy IP address entry to be created in the PDB.
- **probe-target** *ip-address*—(Optional) Specifies an alternate IP address for the probing device to probe. Normally, the probing device transmits a probe to the requesting D-proxy IP address to calculate RTT. If you find that the D-proxy cannot be probed from the probing device, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.
- **zone-data** "*zoneId:RTT*"—(Optional) Specifies the calculated RTT value for a zone, specified in "*zoneId:RTT*" format. For example, enter "**1:100**" to specify zone 3 with an RTT of 100 seconds. Valid entries for *zoneID* are 1 to 32, and must match the proximity zone index specified through the primary GSSM (see the [“Synchronizing the GSS System Clock with an NTP Server”](#) section). Valid entries for the *RTT* value are 0 to 86400 seconds (1 day). To specify multiple static *zone:RTT* pairs in the proximity group, separate each entry within the quotation marks by a comma, but without spaces between the entries (for example, "3:450,22:3890,31:1000").

This example shows how to configure an alternative probing target for the proximity group ISP1:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP1
probe-target 192.168.2.2
```

This example shows how to configure an alternative probing target for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0):

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign ip 192.168.8.0
probe-target 192.168.2.2
```

This example shows how to configure static RTT metrics for the proximity group ISP2 using zone indexes created previously through the primary GSSM:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP2 zone-data
"1:100,2:200,3:300,4:400,5:500"
```

This example shows how to configure static RTT metrics for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0):

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign ip 192.168.8.0
zone-data "1:100,2:200,3:300,4:400,5:500"
```

Deleting Static Entries from the Proximity Database

The GSS allows you to remove entries from the PDB of each GSS device using the CLI. To delete static entries from the PDB in the GSS memory, use the **no** form of the **proximity assign** global server load-balancing configuration mode command.



Note

Ensure that you want to permanently delete static entries from the PDB before you enter the **no proximity assign** command. You cannot retrieve those static entries once they are deleted.

This example shows how to delete static RTT entries for the proximity group ISP1:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no proximity assign group ISP1
zone-data "1:100,2:200,3:300,4:400,5:500"
```

Deleting Entries from the Proximity Database

You can remove PDB entries from the GSS memory by using the **proximity database delete** command. This command, however, does not delete PDB entries saved as part of an automatic dump to a backup file on disk, which the GSS loads upon a reboot or restart to initialize the PDB. To ensure that you successfully remove the desired PDB entries from both GSS memory and disk, enter the **proximity database delete** command followed by the **proximity database periodic-backup now** command to force an immediate backup of the empty PDB residing in GSS memory.

The syntax for this command is as follows:

```
proximity database delete {all | assigned | group {name} | inactive minutes | ip {ip-address} netmask {netmask} | no-rtt | probed}
```

The options and variables are as follows:

- **all**—Removes all proximity database entries from the GSS memory. The prompt “Are you sure?” appears to confirm the deletion of all PDB entries. Specify **y** to delete all entries or **n** to cancel the deletion operation.



Caution

Use the **proximity database delete all** command when you want to remove all entries from the PDB and empty the database. Ensure that you want to permanently delete entries from the PDB before you enter this command since you cannot retrieve PDB entries once you delete them.

- **assigned**—Removes all static entries from the PBD.
- **group** *name*—Removes all entries that belong to a named proximity group. Specify the exact name of a previously created proximity group.
- **inactive** *minutes*—Removes all dynamic entries that have been inactive for a specified time. Valid values are 0 to 43200 minutes.

- **ip** *ip-address netmask netmask*—Removes all proximity entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **no-rtt**—Removes all entries from the PDB that do not have valid RTT values.
- **probed**—Removes all dynamic entries from the PDB.

For example, to remove the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gssm1.example.com# proximity database delete ip 192.168.8.0
255.255.255.0
```

Dumping Proximity Database Entries to a File

The GSS automatically dumps PDB entries to a backup file on the disk approximately every hour. The GSS uses this backup file to initialize the PDB upon system restart or reboot to enable the GSS to recover the contents of the database.

You can dump all or selected entries from the PDB to a named file as a user-initiated backup file. You can then use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the file to a remote machine.

To view the entire contents of a PDB XML output file from the GSS, use the **type** command. See the *Cisco Global Site Selector Administration Guide* for details about displaying the contents of a file.

The GSS includes options that provide a level of granularity for dumping entries from the PDB. The GSS supports binary and Extensible Markup Language (XML) output formats. Optionally, you can specify filters, such as PDB entry type and entry IP network address, to clarify the information dumped from the PDB. PDB entry types can be either statically entered (see the “[Configuring Static Proximity Database Entries](#)” section) or dynamically learned by the GSS. You can instruct the GSS to dump both type of entries from the PDB. If you do not specify an entry type, the GSS automatically dumps all entries from the PDB.

If you attempt to overwrite an existing proximity database dump file with the same filename, the GSS displays the following message:

```
Proximity Database dump failed, a file with that name already exists.
```

To dump entries contained in the PDB to a named file, use the **proximity database dump** command.

The syntax for this command is as follows:

```
proximity database dump {filename} format {binary | xml} [entry-type
{all | assigned | probed}] [entry-address {ip-address} netmask {netmask}]
```

The options and variables are as follows:

- *filename*—Name of the output file that contains the PDB entries on the GSS disk. This file resides in the /home directory.
- **format**—Dumps the PDB entries in binary or XML format. Choose binary encoding as the format type if you intend to load the contents of the file into the PDB of another GSS. The valid entries are as follows:
 - **binary**—Dumps the assigned proximity entries in true binary format. This file can be used only with the **proximity database load** command
 - **xml**—Dumps the assigned proximity entries in XML format. The contents of an XML file include the data fields and the data descriptions. The contents of this file can be viewed using the **type** command. See [Appendix B, “Sticky and Proximity XML Schema Files”](#) for information on defining how content appears in output XML files.



Note

Dumping PDB entries in XML format can be a resource intensive operation and may take from 2 to 4 minutes to complete depending on the size of the PDB and the GSS platform in use. To avoid a degradation in performance, we recommend that you do not perform a PDB dump in XML format during the routine operation of the GSS.

- **entry-type**—Specifies the type of PDB entries to output: static, dynamic, or both. The valid entries are as follows:
 - **all**—Dumps static and dynamic entries from the PDB. This is the default.
 - **assigned**—Dumps statically assigned proximity entries.
 - **probed**—Dumps dynamically probed proximity entries.
- **entry-address** *ip-address*—Specifies the IP address of the PDB entry.
- **netmask** *netmask*—Specifies the subnet mask of the PDB entry in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to dump the dynamic PDB entries to a file named PDB2004_6_30 in XML format. If the dump contains a large number of entries, progress messages may appear.

```
gssm1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Starting Proximity Database dump.
```

```
gssm1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump is in progress...
Proximity Database has dumped 15678 of 34512 entries
```

```
gssm1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump completed. The number of dumped entries: 34512
```

When the dump finishes, a “completed” message displays and the CLI prompt reappears.

Running a Periodic Proximity Database Backup

You can instruct the GSS to dump PDB entries to an output file on the GSS disk before the scheduled time. You may want to initiate a PDB dump as a database recovery method to ensure you store the latest PDB entries before shutting down the GSS.

To force an immediate backup of the PDB residing in GSS memory, use the **proximity database periodic-backup now** command. The GSS sends the PDB entries to the system dump file as the proximity database file. Upon a reboot or restart, the GSS reads this file and loads the contents to initialize the PDB at boot time.

The syntax for this command is as follows:

```
proximity database periodic-backup now
```

For example, enter:

```
gssm1.example.com# proximity database periodic backup now
```

Loading Proximity Database Entries

The GSS enables you to load and merge a PDB from a file into the existing PDB in GSS memory. This PDB merge capability supports the conversion and migration of PDB entries from one GSS into the PDB of another GSS. The file must be in binary format for loading into GSS memory. Proximity RTT metrics loaded from the file replace overlapping entries that exist in the database and supplement the nonoverlapping database entries.

To load a PDB from disk into GSS memory, use the **proximity database load** command. The syntax for this command is as follows:

```
proximity database load filename format binary [override]
```

The options and variable are as follows:

- *filename*—Name of the PDB file to load and merge with the existing PDB on the GSS device. The file must be in binary format for loading into the GSS memory (see the [“Dumping Proximity Database Entries to a File”](#) section). Use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the PDB file to the GSS from a remote GSS.
- **format binary**—Loads the assigned proximity file in true binary format. The file must be in binary format to be loaded into GSS memory.
- **override**—(Optional) Specifies if the proximity database entries in the file are to override the same entries located in the current GSS PDB. When you choose the **override** option, static database entries always have priority over dynamic database entries in the PDB. For the same database entries that exist in both the file and in GSS database memory, the GSS does the following:
 - Overwrites dynamic entries with any overlapping static entries
 - Overwrites static entries with any overlapping static entries, but does not overwrite those entries with any overlapping dynamic entries

If you do not specify the **override** option, the GSS loads the most recent entries into memory, which will replace the older entries of the same type (dynamic or static) in the PDB. For example, the most recent dynamic entries replace the older dynamic entries in the PDB.

This example shows how to load the entries from the GSS3PDB file without overriding the existing entries in the GSS PDB:

```
gssm1.example.com# proximity database load file GSS3PDB format binary
```

For example, to override the same entries located in the existing GSS PDB, enter:

```
gssm1.example.com# proximity database load GSS3PDB format binary
override
```

Initiating Probing for a D-proxy Address

The GSS sends a probe request to each configured probe device in a specified zone to obtain probe information (RTT values). The GSS uses the obtained probe information from the D-proxy to update the PDB entry if the entry can be found in the PDB.

You may need to instruct the probing device in one or all zones (broadcast) to send a probe to a specific D-proxy address, obtain an RTT value, and save the entry in the PDB. To initiate direct probing to a specific D-proxy IP address or direct probing to one or more zones, use the **proximity probe** command.

The syntax for this command is as follows:

```
proximity probe {dproxy_address} [zone {zoneId | all}]
```

The options and variables are as follows:

- *dproxy_address*—IP network address of the D-proxy that you want to probe from the probing device.
- **zone** *zoneId*—Specifies the ID of the proximity zone that contains the probing device from which you want to initiate a probe. Available values are 1 to 32.
- **all**—Specifies that the GSS instruct the probing devices in all configured zones to transmit a probe to the specified D-proxy IP address.

For example, to instruct the probing device in zone 1 to send a probe to the D-proxy at 172.16.5.7, enter:

```
gssm1.example.com# proximity probe 172.16.5.7 zone 1
```

Disabling Proximity Locally on a GSS for Troubleshooting

You can disable proximity for a single GSS when you need to locally override the globally-enabled proximity option to troubleshoot or debug the device. The GSS does not store the local disable setting in its running-config file.

When you enter the **proximity stop** command, the GSS immediately stops the following operations:

- Proximity lookups in the PDB
- Direct probing between the GSS and DRP agents
- Refresh probing to obtain the most up-to-date RTT values
- Periodic PDB dumps
- The proximity database entry age-out process

When you restart the device, the GSS reenables network proximity.

This example shows how to locally disable proximity on a GSS device using the **proximity stop** command:

```
gssm1.example.com# proximity stop
```

This example shows how to locally reenable proximity on a GSS device using the **proximity start** command:

```
gssm1.example.com# proximity start
```

Where to Go Next

[Chapter 10, Configuring DDoS Prevention](#), describes how to configure a GSS to prevent Distributed Denial of Service attacks.



CHAPTER 10

Configuring DDoS Prevention

This chapter describes how to configure a GSS to prevent Distributed Denial of Service (DDoS) attacks. It contains the following major sections:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Enabling or Disabling DDoS Detection and Mitigation](#)
- [Modifying or Restoring Rate Limits](#)
- [Setting a Scaling Factor](#)
- [Configuring Trusted or Spoofed D-proxies](#)
- [Enabling or Disabling Mitigation Rule Checks](#)
- [Configuring a Global Domain Name](#)
- [Configuring Maximum Entries in the DDoS Database](#)
- [Configuring Peacetime Learning](#)
- [Managing Your DDoS Configuration](#)
- [Restoring DDoS Defaults](#)
- [Where to Go Next](#)

Each GSS supports a comprehensive set of **show** CLI commands to display DDoS statistics for the GSS device. In addition, the primary GSSM GUI displays DDoS statistics for the GSS network. See [Chapter 13, Displaying GSS Global Server Load-Balancing Statistics](#), for details about viewing DDoS statistics.

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

To log in and enable privileged EXEC mode in the GSS, you must be a configured user with admin privileges. See the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

To log in to the primary GSSM and enable privileged EXEC mode at the CLI, perform the following steps:

1. If you are remotely logging in to the primary GSSM through Telnet or SSH, enter the hostname or IP address of the GSSM to access the CLI.

If you are using a direct serial connection between your terminal and the GSSM, use a terminal emulation program to access the CLI. For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, see the *Cisco Global Site Selector Getting Started Guide*.

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

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

3. At the CLI prompt, enable privileged EXEC mode as follows:

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

Enabling or Disabling DDoS Detection and Mitigation

You enable the DDoS detection and mitigation module in the GSS by entering the **enable** command in `ddos` configuration mode. The **no** form of this command disables DDoS detection and mitigation. The syntax for this CLI command is as follows:

```
enable
```

Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

**Note**

When you enable DDoS detection and mitigation, the first request of the Boomerang proximity method will not work as expected. All subsequent requests will operate correctly until a D-proxy timeout occurs.

As a workaround, you can specify the D-proxy IP address as trusted on the GSS—even for a first request. For more information, see the [“Configuring Trusted or Spoofed D-proxies”](#) section.

For example:

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

Modifying or Restoring Rate Limits

The GSS enforces a limit on the number of DNS packets per second for each individual D-proxy and an overall global rate limit. It does not enforce a limit for all traffic. You can only configure the rate limit for a particular D-proxy by providing the IP address.

**Note**

The rate-limit is applied to requests entering on port 53 and responses entering on port 5301.

The initial limit value is a default that you can adjust during peacetime learning (see [Configuring Peacetime Learning](#)), or overwrite when you configure either a D-proxy or a group of D-proxies. Once this limit is exceeded, DNS packets are dropped.

**Note**

A time window exists when specifying a rate limit. Thus, if the rate-limit for a particular D-proxy is set to 40, the rate limit will force the GSS to drop packets if the limit is exceeded within 60 seconds from the beginning of the first request.

To configure or modify the rate-limit for a particular D-proxy, or to specify a global rate-limit, enter the **rate-limit** command in ddos configuration mode. The **no** form of this command turns off rate limits.

The syntax for this CLI command is as follows:

```
rate-limit [ipaddress | global | unknown] rate-limit
```

The keywords and arguments for this command are as follows:

- *ipaddress*—IP address of the D-proxy. The default value (per minute) for each D-proxy is 60.
- **global**—Specifies the global rate limit on the GSS. The default value (per minute) is 900000.
- **unknown**—Specifies the rate limit for the D-proxies for which there is no manual entry, or which have not been learned previously. The unknown D-proxy rate-limit ranges from 0-4294967295. By default, the GSS allows 1000 new D-proxies to be added to the database per minute.

**Note**

By configuring the unknown rate-limit, you enable the GSS to handle random spoofed attacks in which there is a flood of unknown D-proxies. When the GSS is under random spoofed attack, new valid D-proxies compete against spoofed D-proxies. In such cases, if the total number of new D-proxies (spoofed and valid) exceeds the unknown rate limit, some valid D-proxies are dropped. However, service to known D-proxies is not affected.

- *rate-limit* —Maximum number of DNS requests the GSS can receive from a D-proxy per second. You must enter absolute values here, such as 1, 2, and 3. You cannot enter fractional values, such as 1.1, 2.2, and 3.3. For the lower limit of the range, you cannot enter a value that is less than 0.

For example, enter:

```
gssm1.example.com(config-ddos)# rate-limit 10.1.1.1 global 10000
gssm1.example.com(config-ddos)#
```

Setting a Scaling Factor

The final rate limits per D-proxy are determined by multiplying the rate-limits learned during peacetime with a scaling factor. To configure this value, enter the **scaling-factor** command in ddos configuration mode. The **no** form of this command turns off the scaling factor for rate limits. The syntax for this CLI command is as follows:

```
scaling-factor d-proxy value
```

The keywords and arguments for this command are as follows:

- **d-proxy**—Specifies the D-proxy scaling factor.
- *value*—Tolerance scaling factor for rate-limiting. You enter the value as a percentage of the rate limit. The default value here is 100.

For example, to change the current rate limit of 10000 to 5000 or 50% of its current value, enter:

```
gssm1.example.com(config-ddos)# scaling-factor d-proxy 50
```

To change that rate limit to 15000 or 150% of its current value, enter:

```
gssm1.example.com(config-ddos)# scaling-factor d-proxy 150
```

Configuring Trusted or Spoofed D-proxies

You can configure trusted or spoofed D-proxies by entering the **dproxy** command in ddos configuration mode. The syntax for this CLI command is as follows:

```
dproxy [trusted ipaddress | spoofed ipaddress]
```

The keywords and arguments for this command are as follows:

- **trusted**—Specifies the D-proxy as trusted.
- **spoofed**—Specifies the D-proxy as spoofed.
- *ipaddress*—IP address of the trusted or spoofed D-proxy.



Note

The entries you add using the CLI will not time out. You can remove these entries only by entering the **no dproxy** command.

For example, enter:

```
gssm1.example.com(config-ddos)# dproxy trusted 10.1.1.1  
gssm1.example.com(config-ddos)#
```

Enabling or Disabling Mitigation Rule Checks

You can enable mitigation rule checks in the GSS by entering the **mitigation-rule** command in ddos configuration mode. The **no** form of this command disables rule checks.



Note

By default, mitigation rule checks are enabled.

The syntax for this CLI command is as follows:

```
mitigation-rule [response | request] enable
```

The keywords and arguments for this command are as follows:

- **response**—Enables or disables the following mitigation rules for DNS responses:
 - Packets are dropped with a source port other than 53 and a QR bit of 1 (response) when responses come from a source port other than 53.
 - Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.
- **request**—Enables or disables the mitigation rules for DNS requests in which packets are dropped with a source port equal to 53, but less than 1024, and a QR bit of 0 (request).

For example, enter:

```
gssm1.example.com(config-ddos)# mitigation-rule response enable  
gssm1.example.com(config-ddos)#
```

Configuring a Global Domain Name

You configure a global domain name by entering the **global-domain** command in ddos configuration mode. You can configure a global domain name to drop all queries, other than the queries for the domains outside the configured domain name.

The syntax for this CLI command is as follows:

```
global-domain domain-name
```

The *domain-name* argument specifies the name of the global domain. The **global-domain** command requires an exact match, so if you enter *.com as a *domain-name*, it does not specify that all domains that are not .com are blocked.

For example, enter:

```
gssml.example.com(config-ddos)# global-domain cisco.com  
gssml.example.com(config-ddos)#
```

**Note**

If a query contains multiple questions, the request is dropped even if one of the questions fails the domain match.

Configuring Maximum Entries in the DDoS Database

You configure the maximum number of entries stored in the DDoS database by entering the **max-database-entries** command in ddos configuration mode.

The syntax for this CLI command is as follows:

```
max-database-entries number
```

The *number* argument specifies the maximum number of entries you wish to store in the GSS database. The range here is from 65536 to 1048576, with a default value of 65536. You can increase or decrease this number to adjust the GSS device.

For example, enter:

```
gssml.example.com(config-ddos)# max-database-entries 1037300  
This command will clear the current DDoS database and create a new  
database with support for 1037300 entries.
```

This command will take effect only after the next `gss stop` and `start`.
Do you want to continue? (y/n):**y**

**Note**

You should use **max-database-entries** only if you wish to clear your current DDoS database and reallocate more or less memory for the DDoS module. After entering the command and executing a `gss stop`, `start`, or `reload`, check the DDoS module status by entering **show ddos status**.

If the command fails and the “Error opening device file” message appears, check the `syslog-messages.log` to determine if a memory allocation failure has occurred. If so, the `syslog-messages.log` reports the following log message: “Unable to allocate sufficient memory for DDoS kernel module. Module insertion failed.” In such cases, you should run **max-database-entries** once more to set a lower value, ignore any error messages that appear, and reboot the GSS.

Executing a Saved DDoS Configuration File

You execute a saved DDoS configuration file by entering the **script play-config** command in DDoS configuration mode.

The syntax for this CLI command is as follows:

```
script play-config filename
```

The *filename* argument specifies the filename of the saved DDoS configuration that you want to execute.

For example, enter:

```
gssml.example.com (config-ddos)# script play-config ddos_config.txt
```

Configuring Peacetime Learning

Different DNS zones may exhibit different behavior. A high traffic rate on one D-proxy may be perfectly normal for another, so a peacetime learning process is required on the GSS. The threshold-tuning phase acquires the baseline or traffic pattern of the specific zone. After these two phases are complete, you can modify zone behavior using the CLI commands.

This section describes the following peacetime learning commands:

- [Starting Peacetime Learning](#)
- [Stopping Peacetime Learning](#)
- [Saving Peacetime Learning](#)
- [Showing Peacetime Learning](#)
- [Erasing Peacetime Learning](#)
- [Setting the Location for the Peacetime File](#)
- [Applying Peacetime Values](#)

Starting Peacetime Learning

You start the peacetime learning process by entering the **ddos peacetime start** command in privileged EXEC mode. This command incrementally updates the values in the peacetime database. If you want to start all over, execute the **ddos peacetime database erase** command before using **ddos peacetime start**. For more information, see the “[Stopping Peacetime Learning](#)” section.

The syntax for this CLI command is as follows:

```
ddos peacetime start
```

For example, enter:

```
gssm1.example.com# ddos peacetime start  
gssm1.example.com#
```

Stopping Peacetime Learning

You stop peacetime learning by entering the **ddos peacetime stop** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
ddos peacetime stop
```

For example, enter:

```
gssml.example.com# ddos peacetime stop  
gssml.example.com#
```

Saving Peacetime Learning

You save peacetime learning to a file on disk by entering the **ddos peacetime save** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
ddos peacetime save filename
```

The *filename* argument specifies the name of the file on disk to which you wish to save peacetime learning.

For example, enter:

```
gssml.example.com# ddos peacetime save  
gssml.example.com#
```

Showing Peacetime Learning

You show the values learned during the peacetime learning process, or the peacetime learning status by entering the **ddos peacetime show** command in privileged EXEC mode.

The syntax for this CLI command is:

```
ddos peacetime show [filename | status]
```

The keywords and arguments for this command are as follows:

- *filename*—Filename of the peacetime learning process for which you want to display values.
- **status**—Shows the current peacetime learning status.

For example, enter:

```
gssml.example.com# ddos peacetime show status  
DDoS Peacetime Learning is not running.
```

Erasing Peacetime Learning

You erase peacetime learning by entering the **ddos peacetime database erase** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
ddos peacetime database erase
```

For example, enter:

```
gssm1.example.com# ddos peacetime database erase  
gssm1.example.com#
```

Setting the Location for the Peacetime File

You set the location or file that the peacetime file uses in a **ddos peacetime apply** operation by entering the **peacetime database** command in **ddos** configuration mode. The peacetime database location is specified when you use the **peacetime database** command

The syntax for this CLI command is as follows:

```
peacetime database file
```

The *file* argument specifies the peacetime file to use.



Note

If you do not configure a location for the peacetime file, or if you enter the **no peacetime database** command, the result is that the peacetime database is used from system memory.

For example, enter:

```
gssm1.example.com(config-ddos)# peacetime database samplefile  
gssm1.example.com(config-ddos)#
```

Applying Peacetime Values

You apply values learned during the peacetime learning process to the rate-limit database by entering the **ddos peacetime apply** command in privileged EXEC mode. This command updates the rate-limit database with the peacetime learned values.

The peacetime database location is specified in the **peacetime database** command. If you do not specify this command, the in-memory database is used instead.

The syntax for this CLI command is as follows:

```
ddos peacetime apply [increment | overwrite]
```

The keywords and arguments for this command are as follows:

- **increment**—Specifies that you want to apply the peacetime learned values incrementally to the database.
- **overwrite**—Specifies that you want to restore all the values in the rate-limit database to their defaults and then update them with the values learned during peacetime.

For example, enter:

```
gssm1.example.com# ddos peacetime apply increment  
gssm1.example.com#
```

Managing Your DDoS Configuration

Two commands are available that allow you to manage your DDoS configuration. This section describes the following topics:

- [Copying a DDoS Configuration to Disk](#)
- [Clearing a DDoS Configuration](#)

Copying a DDoS Configuration to Disk

You copy the DDoS configuration to disk by entering the **copy ddos-config** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
copy ddos-config disk filename
```

The **disk filename** keyword and argument indicate that you want to copy the configuration to disk and store it under the specified file name.

For example, enter:

```
gssm1.example.com# copy ddos-config disk ddos_config.txt  
gssm1.example.com#
```

Clearing a DDoS Configuration

You clear a DDoS configuration by entering the **ddos-configuration** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
clear ddos-config
```

For example, enter:

```
gssm1.example.com# clear ddos-config  
gssm1.example.com#
```

Restoring DDoS Defaults

You restore the default values in the rate-limit database by entering the **ddos restore-defaults** command in privileged EXEC mode.

The syntax for this CLI command is as follows:

```
ddos restore-defaults ipaddress
```

The *ipaddress* argument specifies the D-proxy IP address and indicates that you wish to restore the rate limit of the designated D-proxy to the default rate and the state to Unknown.

For example, enter:

```
gssm1.example.com# ddos restore-defaults 1.1.1.2
```

Where to Go Next

[Chapter 11, Creating and Playing GSLB Configuration Files](#), describes how to create, modify, and play (execute) GSLB configuration files.



CHAPTER 11

Creating and Playing GSLB Configuration Files

This chapter describes how to create, modify, and play (execute) GSLB configuration files. GSLB configuration files define all global server load-balancing configuration parameters for a GSS network, including the parameters that define resources, domains, source addresses, answers, keepalives, DNS rules, sticky, and proximity properties.

Using the CLI, you can quickly create a GSLB configuration file from an existing GSS network that has been configured for global server load balancing. If desired, you can modify the GSLB configuration file using a text editor. Playing the GSLB configuration file on a new or previously configured GSS network automatically updates its global server load-balancing configuration.

This chapter contains the following major sections:

- [GSLB Configuration File Overview](#)
- [Creating a GSLB Configuration File](#)
- [Securely Copying GSLB Configuration Files](#)
- [Modifying a GSLB Configuration File](#)
- [Playing a GSLB Configuration File](#)
- [Where to Go Next](#)

GSLB Configuration File Overview

The ability to create and play global server load-balancing configuration files is particularly useful in the following situations:

- You have an existing GSS network that is successfully configured for global server load balancing and you need to develop a new, second GSS network. In most cases, creating a GSLB configuration file on the existing network and playing it on the new network will be significantly more efficient than developing a new global server load-balancing configuration.
- You need to transfer the domain and source address lists from one GSS network to another. Rather than manually entering multiple domains and source addresses, you can quickly copy them from the GSLB configuration file of a source GSS network to the GSLB configuration file of a target GSS network, and then play the updated file to load the new data onto the target network.
- You have two GSS networks, for example, GSS1 and GSS2. You would like to use much of the global server load-balancing development that has occurred for the GSS1 network on your GSS2 network. You realize that playing the GSLB configuration file from the GSS1 network on the GSS2 network will likely generate errors (due to conflicting data), but the ability to edit and replay the configuration file to address the errors provides the easiest path to update the GSS2 network.
- You have a DistributedDirector-based network that you are planning to transition over to a GSS network. To save time, you want to import host, domain, and source address information from the DistributedDirector network to the GSS network. You can do this by creating GSLB configuration text files on both the DistributedDirector and GSS systems, copying the pertinent information from the Cisco IOS-based file to the GSS file, modifying the new information to conform to GSS requirements, and then playing the updated file on the primary GSSM.

Creating a GSLB Configuration File

You create a GSLB configuration file that you can modify and import to a new or previously configured GSS network by using the **copy gslb-config** command in privileged EXEC mode. Use this file to automatically update its global server load-balancing configuration.

The syntax of this command is as follows:

```
copy gslb-config disk filename
```

The *filename* argument is the name of the output file that contains the GSLB configuration. Enter the filename only. Do not include the path information with the filename. The file is copied to the root directory on the primary GSSM.

For example, to create a GSLB configuration file named `GSLB_CONFIG_1.txt`, enter:

```
gssm1.example.com# copy gslb-config disk GSLB_CONFIG_1.TXT  
gssm1.example.com#
```

To verify that the file is copied to disk on the GSSM by using the **dir**, **ls**, or **lls** commands in privileged EXEC mode, enter:

```
gssm1.example.com# ls  
...  
GSLB_CONFIG_1.TXT  
...  
gssm1.example.com#
```

See the “Displaying Files in a Directory” section in Chapter 2, Managing the GSS from the CLI, in the *Cisco Global Site Selector Administration Guide* for more information on the **dir**, **ls**, and **lls** commands.

**Note**

You can also use the **show gslb-config>filename** command to redirect the current GSLB configuration to a file (specified by the *filename* variable). The file is copied to the root directory of the primary GSSM. See the “Controlling Command Output” section in Chapter 1, Command-Line Interface Command Summary, in the *Cisco Global Site Selector Administration Guide* for details about using the redirect (>) character.

You can view the contents of the current global server load-balancing configuration used by the GSS network by entering the **show gslb-config** command. This command displays information on all GSLB parameters, including resources, domains and domain lists, source addresses and source address lists, answers and answer groups, keepalives, DNS rules, sticky and proximity properties.

Securely Copying GSLB Configuration Files

You copy a GSLB configuration file from one primary GSSM to another by using the **scp** command in privileged EXEC mode.



Note

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

To securely copy files from the GSSM where you are currently logged in to another GSSM, use the **scp** command. The syntax is as follows:

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

To securely copy files from another GSSM to the GSSM where you are currently logged in, use the **scp** command. The syntax is as follows:

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

For example, to copy the GSLB configuration file named `GSLB_CONFIG_1.txt` on the primary GSSM where you are currently logged in to another primary GSSM, enter:

```
gssm1.example.com# scp GSLB_CONFIG_1.TXT myusername@192.168.2.3:/home  
gssm1.example.com#
```

For more information on the **scp** command, see the “Securely Copying Files” section in Chapter 2, Managing the GSS from the CLI, in the *Cisco Global Site Selector Administration Guide*.

Modifying a GSLB Configuration File

After you create a GSLB configuration file, you can use a text editor to modify it as needed before playing the file on a GSS network. You should review the following topics before modifying a GSLB configuration file:

- [File Modification Guidelines](#)
- [File Modification Workflow](#)

File Modification Guidelines

Follow these guidelines when modifying a GSLB configuration file:

- When modifying a GSLB configuration file from one network for play on another network, and you have specified sticky mesh peer names, you must modify the **favored-peer** GSS device names for use on the new network (where the two networks use different hostnames). See the “[Configuring DNS Sticky](#)” section of [Chapter 8, “Configuring DNS Sticky](#)” for details about the **favored-peer** command.
- Each line in the configuration file must contain a single command followed by a carriage return.
- Extra spaces are ignored when the file is played.
- Commands that create objects must appear before commands that refer to those objects.
- Lower-level commands (for example, the **favored-peer** command in the sticky properties configuration mode) must follow their respective higher level command (for example, the **sticky-properties** command in GSLB configuration mode).
- Do not use the **config** and **gslb** commands to enter the global configuration and gslb configuration modes. These actions are implied and automatically executed by the **script play-config** command.
- Do not use the **exit** command at the end of the file. Exiting is implied and is automatically executed.

- The use of the “?” wildcard for entering hosted domain names is allowed in GSLB configuration files. However, the “?” wildcard is not allowed when using the **domain** command to enter hosted domain names. See the [“Configuring Domain Lists”](#) section in [Chapter 4, Configuring Domain Lists](#) for more information about entering domain names.

File Modification Workflow

To copy all source address lists and associated addresses and all domain lists and associated domain names from a GSLB configuration file from the GSS1 network to the GSS2 network, perform the following steps:

1. Execute a backup at the primary GSSM for both GSS1 and GSS2 networks.
2. At the primary GSSM of both GSS1 and GSS2 networks, enter the **copy gslb-config disk** command to create separate, uniquely named GSLB configuration files. See the [“Creating a GSLB Configuration File”](#) section for details about the **copy gslb-config disk** command.
3. At the primary GSSM for the GSS2 network, enter the **scp** command to copy the GSLB configuration file created on the GSS1 network to the primary GSSM on the GSS2 network. See the [“Securely Copying GSLB Configuration Files”](#) section for details about using the **scp** command.
4. Open both GSLB configuration files in a text editor.
5. Copy the domain lists and associated domain names and source address lists and associated addresses from the configuration file created for the GSS1 network, and then paste them into the configuration file created for the GSS2 network.
6. Save the modified GSLB configuration file for the GSS2 network.
7. At the primary GSSM for the GSS2 network, enter the **script play-config** command in global server load-balancing configuration mode to play the modified file and import the new domain and source address data. See the [“Playing a GSLB Configuration File”](#) section for more information about using the **script play-config** command.

Playing a GSLB Configuration File

You play a GSLB configuration file by entering the **script play-config** command in global server load-balancing configuration mode.

**Note**

If the size of the static proximity group configuration is very large, we recommend that you use the **proximity play-config** command instead since it plays the proximity commands more efficiently.

The syntax of this command is as follows:

```
script play-config filename
```

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

**Note**

Executing the **script play-config** command overwrites existing duplicate GSLB commands on the primary GSSM.

For example, to play the GSLB configuration file named `GSLB_CONFIG_1.txt`, enter:

```
gssm1.example.com(config-gslb)# script play-config GSLB_CONFIG_1.TXT
```

If any errors are encountered with a command line, they are displayed and the file continues to play to completion. Any additional command line errors that are encountered are also displayed as follows:

```
gssm1.example.com(config-gslb)# script play-config GSLB_CONFIG_1.TXT  
ERROR:Unable To Perform Source-Address-List Operation.Please Configure  
Owner Prior To Source-Address-List  
ip address 192.168.10.1 255.255.255.0  
  
% Invalid input detected at '^' marker.  
ip address 192.168.10.6 255.255.255.255  
^  
  
% Invalid input detected at '^' marker.  
gssm1.example.com(config-gslb)#
```

In this example, the specified owner for the two listed IP addresses that are assigned to a source address list was not configured on the target GSS network. You can correct this problem in one of two ways:

- Change the name of the owner in the GSLB configuration file to reflect a configured owner name, and then replay the file using the **script play-config** command.
- If appropriate, add the owner name to the configuration using the **owner** command, and then replay the file using the **script play-config** command.

To view additional information for errors encountered during a play, use the **show gslb-errors** command in privileged EXEC mode.

For example, enter:

```
gssm1.example.com# show gslb-errors
GSLB-CLI-PLAY-CONFIG [Thu Dec 8 17:09:54 2005]:STARTING PLAY-CONFIG
MESSAGE LOGGING
GSLB-CLI-PLAY-CONFIG [Thu Dec 8 17:09:57 2005]:ERROR: Could Not
Perform Source-Address-List Operation.Object
/source-address-list/owner:OWNER1 Not Configured.
GSLB-CLI-PLAY-CONFIG [Thu Dec 8 17:10:01 2005]:STOPPING PLAY-CONFIG
MESSAGE LOGGING

gssm1.example.com#
```

Where to Go Next

[Chapter 12, Displaying Global Server Load-Balancing Configuration Information](#), describes the **show gslb-config** commands that allow you to display GSS resource, domain, keepalive, answer, dns rule, sticky, and proximity information.



CHAPTER 12

Displaying Global Server Load-Balancing Configuration Information

The GSS provides a comprehensive set of **show gslb-config** commands that display GSS global server load-balancing configuration information. These commands allow you to display resource, domain, keepalive, answer, dns rule, sticky, and proximity information for your GSS configuration. The **show gslb-config** commands are available in all CLI modes except interface configuration mode.

This chapter contains the following major sections:

- [Displaying Resource Configuration Information](#)
- [Displaying Source Address Configuration Information](#)
- [Displaying Domain Configuration Information](#)
- [Displaying Keepalive Configuration Information](#)
- [Displaying Shared Keepalive Configuration Information](#)
- [Displaying Answer Configuration Information](#)
- [Displaying Answer Group Configuration Information](#)
- [Displaying DNS Rule Configuration Information](#)
- [Displaying DNS Sticky Configuration Information](#)
- [Displaying DNS Proximity Configuration Information](#)
- [Where to Go Next](#)

Displaying Resource Configuration Information

You display configuration information about GSS locations, owners, regions and zones by using the **show gslb-config location**, **show gslb-config owner**, **show gslb-config region** and **show gslb-config zone** commands.

Displaying Location Configuration Information

You display information for the currently configured locations on the GSS by using the **show gslb-config location** command.

The syntax for the **show gslb-config location** command is as follows:

```
show gslb-config location [location_name]
```

The *location_name* argument specifies the name of a previously created location. Enter the variable as a case-sensitive, unquoted text string.

[Table 12-1](#) describes the fields in the **show gslb-config location** command output.

Table 12-1 Field Descriptions for show gslb-config location Command

Field	Description
Location	Name of the location.
Region	Region associated with the location.
Zone	Zone associated with the location.
Comments	Comments about the location.

Displaying Owner Configuration Information

You display information for the currently configured owners on the GSS by using the **show gslb-config owner** command.

The syntax for the **show gslb-config owner** command is as follows:

```
show gslb-config owner [owner_name]
```

The *owner_name* argument specifies the name of a previously created owner. Enter the variable as a case-sensitive, unquoted text string.

Table 12-2 describes the fields in the **show gslb-config owner** command output.

Table 12-2 Field Descriptions for show gslb-config owner Command

Field	Description
Owner	Name of the owner.
Comments	Comments about the owner.

Displaying Region Configuration Information

You display information for the currently configured regions on the GSS by using the **show gslb-config region** command.

The syntax for the **show gslb-config region** command is as follows:

```
show gslb-config region [region_name]
```

The *region_name* argument specifies the name of a previously created region. Enter the variable as a case-sensitive, unquoted text string.

Table 12-3 describes the fields in the **show gslb-config region** command output.

Table 12-3 Field Descriptions for show gslb-config region Command

Field	Description
Region	Name of the region.
Comments	Comments about the region

Displaying Zone Configuration Information

You display information for the currently configured zones on the GSS by using the **show gslb-config zone** command.

The syntax for the **show gslb-config zone** command is as follows:

```
show gslb-config zone [zone_name]
```

The *zone_name* argument specifies the name of a previously created zone. Enter the variable as a case-sensitive, unquoted text string.

Table 12-4 describes the fields in the **show gslb-config zone** command output.

Table 12-4 Field Descriptions for show gslb-config zone Command

Field	Description
Zone	Name of the zone.
Backup IP address	IP address of the backup probe device servicing the zone.
Index	Numerical identifier for the zone.
Probe IP address	IP address of the primary probe device servicing the zone.

Displaying Source Address Configuration Information

You display configuration information about GSS source address lists and source addresses by using the **show gslb-config source-address-list** command.

The syntax for this command is as follows:

```
show gslb-config source-address-list [source-address-list_name]
```

The *source-address-list_name* argument specifies the name of a previously created source address list. Enter the variable as a case-sensitive, unquoted text string.

Table 12-5 describes the fields in the **show gslb-config source-address-list** command output.

Table 12-5 Field Descriptions for `show gslb-config source-address-list` Command

Field	Description
Source address list	Name of the source address list.
Owner	Owner name associated with the source address list.
IP addresses	IP addresses or CIDR address blocks of the client DNS proxies for the source address list.
Comments	Comments about the source address list.

Displaying Domain Configuration Information

You display configuration information about GSS domain lists and domains by using the `show gslb-config domain-list` command.

The syntax for this command is as follows:

```
show gslb-config domain-list [domain-list_name]
```

The *domain-list_name* argument specifies the name of a previously created domain list. Enter the variable as a case-sensitive, unquoted text string.

[Table 12-6](#) describes the fields in the `show gslb-config domain-list` command output.

Table 12-6 Field Descriptions for `show gslb-config domain list` Command

Field	Description
Domain address list	Name of the domain list.
Owner	owner name associated with the domain list.
Domains	Names of hosted domains that are part of the domain list and for which the GSS acts as the authoritative DNS server.
Comments	Comments about the domain list.

Displaying Keepalive Configuration Information

You display configuration information about GSS keepalive properties by using the **show gslb-config keepalive-properties** command. The displayed output shows the currently configured properties for ICMP, TCP, HTTP HEAD, KAL-AP, CRA, and NS type keepalives. Both Fast and Standard failure detection mode properties are displayed for ICMP, TCP, HTTP HEAD, KAL-AP, and Scripted Kal keepalive types.

The syntax for this command is as follows:

```
show gslb-config keepalive-properties
```

[Table 12-7](#) describes the fields in the **show gslb-config keepalive-properties** command output.

Table 12-7 *Field Descriptions for show gslb-config keepalive-properties Command*

Field	Description
ICMP Keepalives—Standard Failure Detection Mode	
interval min	Value that specifies the minimum frequency with which the GSS attempts to schedule ICMP keepalives.
ICMP Keepalives—Fast Failure Detection Mode	
retries	Value that specifies the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline.
successful probes	Number of consecutive successful ICMP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online.
TCP Keepalives—Standard Failure Detection Mode	
port	Port on the remote device that is to receive the TCP-type keepalive request from the GSS.
termination	Method that the GSS initiates to close a TCP connection (graceful or reset).

Table 12-7 Field Descriptions for *show gslb-config keepalive-properties* Command (continued)

Field	Description
timeout	Length of time allowed before the GSS retransmits data to a device that is not responding to a request.
interval min	Minimum frequency with which the GSS attempts to schedule TCP keepalives.
TCP Keepalives—Fast Failure Detection Mode	
port	Port on the remote device that is to receive the TCP-type keepalive request from the GSS.
termination	Method that the GSS initiates to close a TCP connection (graceful or reset).
retries	Number of times that the GSS retransmits a TCP packet before declaring the device offline.
successful probes	Number of consecutive successful TCP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online.
HTTP HEAD Keepalives—Standard Failure Detection Mode	
port	Port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS.
path	Server website queried in the HTTP HEAD request (for example, /company/owner).
termination	Method that the GSS initiates to close an HTTP HEAD connection (graceful or reset).
timeout	Length of time allowed before the GSS retransmits data to a device that is not responding to a request.
interval min	Minimum frequency with which the GSS attempts to schedule HTTP HEAD keepalives.
HTTP HEAD Keepalives—Fast Failure Detection Mode	
port	Port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS.
path	Server website queried in the HTTP HEAD request (for example, /company/owner).

Table 12-7 Field Descriptions for *show gslb-config keepalive-properties* Command (continued)

Field	Description
termination	Method that the GSS initiates to close an HTTP HEAD connection (graceful or reset).
interval min	Minimum frequency with which the GSS attempts to schedule HTTP HEAD keepalives.
KAL-AP Keepalives—Standard Failure Detection Mode	
capp-key	Secret key to be used for Content and Application Peering Protocol (CAPP) encryption.
interval min	Minimum frequency with which the GSS attempts to schedule KAL-AP keepalives.
KAL-AP Keepalives—Fast Failure Detection Mode	
capp-key	Secret key to be used for Content and Application Peering Protocol (CAPP) encryption.
retries	Number of times that the GSS retransmits an KAL-AP packet before declaring the device offline.
successful probes	Number of consecutive successful KAL-AP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online.
Scripted Kal Keepalives—Standard Failure Detection Mode	
interval min	Value that specifies the minimum frequency with which the GSS attempts to schedule Scripted Kal keepalives.
Scripted Kal Keepalives—Fast Failure Detection Mode	
retries	Value that specifies the number of times that the GSS retransmits a Scripted keepalive request packet before declaring the device offline.
successful probes	Number of consecutive successful Scripted Kal keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online.

Table 12-7 Field Descriptions for *show gslb-config keepalive-properties* Command (continued)

Field	Description
CRA Keepalives	
cra-timing-decay	Value that the GSS uses to weigh recent DNS Round Trip Time (RTT) probe results relative to earlier RTT metrics.
interval min	Minimum frequency with which the GSS attempts to schedule CRA keepalives.
Name Server Keepalives	
query-domain	Name of the domain name server to which an NS-type keepalive is sent.
interval min	Minimum frequency with which the GSS attempts to schedule NS keepalives.

Displaying Shared Keepalive Configuration Information

You display configuration information about shared keepalives by using the **show gslb-config shared-keepalive** command. The displayed output shows the currently configured properties for ICMP, TCP, HTTP HEAD, KAL-AP, and Scripted keepalive shared keepalives.

The syntax for this command is as follows:

```
show gslb-config shared-keepalive [ip_address]
```

The *ip_address* argument specifies the IP address that was specified for any previously configured shared keepalives.

[Table 12-8](#) describes the fields in the **show gslb-config shared-keepalive** command output.

Table 12-8 *Field Descriptions for show gslb-config shared-keepalive Command*

Field	Description
ICMP Shared Keepalives	
ip_address	IP address used to test the online status for the linked VIP.
TCP Shared Keepalives	
ip_address	IP address used to test the online status for the linked VIP.
port	Port on the remote device that is to receive the TCP-type keepalive request from the GSS.
termination	Method that the GSS initiates to close a TCP connection (graceful or reset).
HTTP Shared Keepalives	
ip_address	IP address used to test the online status for the linked VIP.
port	Port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS.
host tag	Domain name that is sent to the VIP as part of the HTTP HEAD query.
path	Path that is relative to the server website being queried in the HTTP HEAD request.
KAL-AP Shared Keepalives	
ip_address	IP address used to test the online status for the linked VIP.
secondary ip_address	IP address used to query a second Cisco CSS or CSM in a virtual IP (VIP) redundancy and virtual interface redundancy configuration.
capp-secure enable	Indicates whether the capp-secure option is enabled. This option must be enabled if you intend to use Content and Application Peering Protocol (CAPP) encryption.

Table 12-8 Field Descriptions for `show gslb-config shared-keepalive` Command (continued)

Field	Description
key	Encryption key that is used to encrypt interbox communications using CAPP.
retries	Number of times that the GSS retransmits an KAL-AP packet before declaring the device offline. Applicable only for Fast failure detection mode.
successful probes	Number of consecutive successful KAL-AP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online. Applicable only for Fast failure detection mode.
Scripted Kal Shared Keepalives	
ip_address	IP address used to test the online status for the linked VIP.

Displaying Answer Configuration Information

You display the current property settings for configured answers by using the `show gslb-config answer` command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
show gslb-config answer [ip_address {type} | name]
```

The variables for this command are as follows:

- *ip_address*—(Optional) Answers that specify the IP address. Enter an unquoted text string in dotted-decimal format.
- *type*—Answer type for the specified IP address. Valid options are as follows:
 - **cra**—Specifies a CRA-type answer
 - **ns**—Specifies an NS-type answer
 - **vip**—Specifies a VIP-type answer
- *name*—(Optional) Answer that uses the specified name.

Table 12-9 describes the fields in the `show gslb-config answer` command output for VIP-, CRA- and NS-type answers.

Table 12-9 Field Descriptions for show gslb-config answer Command

Field	Description
Output for VIP-Type Answers	
type	Answer type (VIP).
ip_address	VIP address field for the answer. This is the VIP address to which the GSS will forward requests.
name	Optional name for the answer.
location	Optional location name to which the answer is associated.
active/suspend	Current state of the answer (active or suspend).
keepalive type (and configuration information)	Type of keepalive (ICMP, TCP, HTTP HEAD, KAL-AP, or Scripted Kal). See the “Displaying Keepalive Configuration Information” section for output details for these keepalive types.
Output for CRA-Type Answers	
type	Answer type (CRA).
ip_address	Interface or circuit address of the CRA.
name	Optional name for the answer.
location	Optional location name to which the answer is associated.
enable/disable	Enable indicates that the GSS is to perform keepalive checks on the answer. Disable indicates that the GSS uses a one-way delay to calculate a static RTT.
delay	One-way delay time in milliseconds that is used by the GSS to calculate a static round-trip time (RTT).
active/suspend	Current state of the answer (active or suspend).
Output for Name Server-Type Answers	
type	Answer type (NS).
ip_address	Name server that the GSS is to forward its requests.

Table 12-9 Field Descriptions for *show gslb-config answer* Command

Field	Description
name	Optional name for the answer.
enable/disable	Enable indicates that the GSS is to perform keepalive checks on the name server. Disable indicates that the GSS assumes that the name server is always online.
domain	Name of the domain name server to which an NS-type keepalive is sent (to determine the online status).
active/suspend	Current state of the answer (active or suspend).

Displaying Answer Group Configuration Information

You display the current property settings for configured answers by using the **show gslb-config answer-group** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
show gslb-config answer-group [name]
```

The *name* variable specifies the name of a specific answer group.

[Table 12-10](#) describes the fields in the **show gslb-config answer-group** command output for VIP-, CRA- and NS-type answers.

Table 12-10 Field Descriptions for *show gslb-config answer group* Command

Field	Description
type	Answer group type (CRA, NS, or VIP).
name	Optional name for the answer group.
owner	Optional owner name to which the answer group is associated.

Displaying DNS Rule Configuration Information

You display the current property settings for all configured dns rules and balance clauses for each rule by using the **show gslb-config dns rule** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

```
show gslb-config dns rule [name]
```

The *name* argument specifies the name of a previously created dns rule.

[Table 12-11](#) describes the fields in the **show gslb-config dns rule** command output. Output for balance clauses that use VIP-, NS-, and CRA-type answer groups is also shown.

Table 12-11 Field Descriptions for show gslb-config dns rule Command

Field	Description
dns rule name	Name of the DNS rule.
owner	Name of the owner with whom the rule is associated.
source address list	Name of the source address list from which requests originate.
domain list	Name of the domain list to which DNS queries are addressed.
query	DNS query type (a or all) that is applied to the rule.
sticky method	Displays how (by domain or domain list) the GSS supports DNS stickiness in a DNS rule.
timeout	Time interval that can pass without the sticky database receiving a lookup request for an entry. This value overrides the global value (for this DNS rule).

Output for Balance Clauses that Use VIP-Type Answer Groups

clause number	Balance Clause number (1, 2, or 3)
vip-group name	Name of the answer group specified for the clause.
method	Method type for the balance clause: (round-robin , least-loaded , ordered , weighted-round-robin , or hashed)

Table 12-11 Field Descriptions for *show gslb-config dns rule* Command (continued)

Field	Description
ttl number	Duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer.
count number	Duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer.
Output for Balance Clauses that Use NS-Type Answer Groups	
clause number	Balance Clause number (1, 2, or 3)
vip-group name	Name of the answer group specified for the clause.
method	Method type for the balance clause: (round-robin, ordered, weighted-round-robin, or hashed)
Output for Balance Clauses that Use CRA-Type Answer Groups	
clause number	Balance Clause number (1 or 2)
vip-group name	Name of the answer group specified for the clause.
ttl number	Duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer.
fragment number	Number of address records (A-records) that the GSS to returns for requests that match the DNS rule.
ip-ttl number	Maximum number of network hops that are utilized when returning a response to a CRA from a match on a DNS rule.
max-prop-delay number	Maximum propagation delay (in milliseconds) that is observed before the boomerang server component of the GSS forwards a DNS request to a CRA.
method boomerang	DNS rule that uses a boomerang DNS race to determine the best site.
pad	Amount of extra data (in bytes) included with each CRA response packet.

Table 12-11 Field Descriptions for *show gslb-config dns rule* Command (continued)

Field	Description
secret key	Key used to encrypt critical data sent between the GSS boomerang server and CRAs.
server-delay number	Maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS returns the address of its “last gasp” server as a response to the requesting name server.

Displaying DNS Sticky Configuration Information

You display global sticky group and global sticky property information by using the **show gslb-config sticky-group** and **show gslb-config sticky-properties** commands. To display sticky method information for currently configured DNS rules, see the “[Displaying Answer Configuration Information](#)” section.

Displaying Global Sticky Group Information

Display global sticky group information by using the **show gslb-config sticky-group** command.

The syntax for this command is as follows:

```
show gslb-config sticky-group [name]
```

The *name* argument specifies the name of a previously created sticky group.

[Table 12-12](#) describes the fields in the **show gslb-config sticky-group** command output.

Table 12-12 Field Descriptions for *show gslb-config sticky-group* Command

Field	Description
name	Name of the previously created sticky group

Table 12-12 Field Descriptions for show gslb-config sticky-group Command

Field	Description
ip_address	IP address of the sticky group.
netmask	Netmask of the sticky group.

Displaying Global Sticky Properties Information

You display information about global sticky settings by using the **show gslb-config sticky-properties** command.

The syntax for this command is as follows:

```
show gslb-config sticky-properties
```

[Table 12-13](#) describes the fields in the **show gslb-config sticky-properties** command output.

Table 12-13 Field Descriptions for show gslb-config sticky-properties Command

Field	Description
enable	Stickiness enable state (global or local).
mask netmask	Global subnet mask value that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of clients that the sticky database can support.
timeout	Value for the maximum time period that an unused answer remains valid in the sticky database.

Displaying DNS Proximity Configuration Information

You display global proximity group and global proximity property information by using the **show gslb-config static-proximity** and **show gslb-config proximity-properties** commands.

Displaying Global Proximity Group Information

You display global proximity group information by using the **show gslb-config static-proximity** command.

The syntax for this command is as follows:

```
show gslb-config static-proximity [name]
```

The *name* argument specifies the name of a previously created proximity group.

[Table 12-14](#) describes the fields in the **show gslb-config static-proximity** command output.

Table 12-14 Field Descriptions for show gslb-config static-proximity Command

Field	Description
name	Name of the previously created proximity group.
ip_address	IP address for the proximity group.
netmask	Netmask for the proximity group.

Displaying Global Proximity Properties Information

You display information about global proximity settings by using the **show gslb-config proximity-properties** command.

The syntax for this command is as follows:

```
show gslb-config proximity-properties
```

[Table 12-15](#) describes the fields in the **show gslb-config proximity-properties** command output.

Table 12-15 Field Descriptions for show gslb-config sticky-properties Command

Field	Description
enable	Global proximity enable state.
mask netmask	Global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of supported D-proxies in the PDB.
timeout minutes	Maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry.
equivalence number	Percentage value that the GSS applies to the most proximate RTT value (the closest) to identify the relative RTT values of other zones that the GSS should consider as equally proximate.
refresh-interval hours	Frequency of the refresh probing process to probe and update RTT values for the entries in the PDB.
discovery-sequence	Type of probe method used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy.
acceptable-rtt number	Value that the GSS uses as an acceptable RTT value when determining the most proximate answer.
acceptable-zone number	Percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values.
wait enable	Wait enable state. When enabled, the GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings.
authentication drp enable	Authentication drp enable state. When enabled, the GSS authenticates packets that it exchanges with the DRP agent in a probing device through the exchange of DRP keys.
key drp	All configured DRP key ID numbers and names.

Where to Go Next

[Chapter 13, Displaying GSS Global Server Load-Balancing Statistics](#), describes the tools that allow you to display the status of global server load balancing on your network, including the CLI commands and the GSSM GUI monitor pages.



CHAPTER 13

Displaying GSS Global Server Load-Balancing Statistics

This chapter describes the following tools for displaying the status of global server load balancing on your GSS network:

- CLI-based commands that display the content routing and global server load-balancing statistics performed by a GSS device (primary GSSM, standby GSSM, and GSS device).
- Monitor pages in the primary GSSM GUI that display the status of global server load-balancing activity for all GSS devices in your GSS network.

This chapter contains the following major sections:

- [Displaying Global Server Load-Balancing Statistics from the CLI](#)
- [Displaying Global Server Load-Balancing Statistics from the GUI](#)

Displaying Global Server Load-Balancing Statistics from the CLI

Each GSS device includes a comprehensive set of **show statistics** CLI commands to display content routing and load-balancing statistics for each major component involved in the GSS global server load-balancing operation. The GSS global server load-balancing components include boomerang (CRAs), DNS, and VIP keepalives. For example, the **show statistics dns** command can be used to display the traffic handled by a particular DNS rule, which matches a D-proxy to an answer, or to analyze the traffic to a particular hosted domain that is managed by a GSS.

You can also display advanced traffic management functions such as DNS sticky and network proximity for the GSS device.

The following topics provide detailed instructions about using the output of the various **show statistics** command options to display GSS global server load-balancing operation:

- [Displaying the Status of the Boomerang Server on a GSS](#)
- [Displaying the Status of the DNS Server on a GSS](#)
- [Displaying the Status of the DRP Agent on a GSS](#)
- [Displaying DDoS Statistics on a GSS](#)
- [Displaying the Status of Keepalives on a GSS](#)
- [Displaying DNS Sticky Statistics on a GSS](#)
- [Clearing GSS Global Server Load-Balancing Statistics](#)

Displaying the Status of the Boomerang Server on a GSS

The boomerang server component uses calculations of network delay, provided by DNS races between content routing agents (CRAs), to determine which server is best able to respond to a given request. Use the **show statistics boomerang** command to display boomerang activity, such as DNS races, on your GSS device on a domain-by-domain basis or on a global basis.

The syntax for the **show statistics boomerang** command is as follows:

```
show statistics boomerang { domain domain_name | global }
```

The keywords and arguments are as follows:

- **domain**—Displays statistics related to a named domain being served by the GSS.
- *domain_name*—Name of the domain.
- **global**—Displays statistics across the entire GSS network for the Boomerang server.

This example shows how to displays statistics across the entire GSS network for the boomerang server:

```
gss1.yourdomain.com# show statistics boomerang global  
Boomerang global statistics:  
    Total races: 24
```

This example shows how to displays boomerang statistics for a specific domain:

```
gss1.yourdomain.com# show statistics boomerang domain1  
Domain statistics: (of domain1)  
    DNS A requests:
```

Displaying the Status of the DNS Server on a GSS

The DNS server component tracks all DNS-related traffic to and from your GSS device, including information about DNS queries received, responses sent, queries dropped and forwarded. Use the **show statistics dns** command option to display DNS statistics about your GSS request routing and server load-balancing components such as DNS rules, answers, answer groups, domains, domain lists, proximity lookups by rule name or zone, source addresses, and source address groups.

When displaying the DNS answer group, domain list, or source address list statistics, you may specify the **verbose** option to display detailed statistics about each component of your DNS rules (for example, statistics for each answer that makes up an answer group or each domain that makes up a domain list).

This section contains the following topics:

- [Displaying Answer Statistics](#)
- [Displaying Answer Group Statistics](#)
- [Displaying Domain Statistics](#)
- [Displaying Domain List Statistics](#)
- [Displaying Global Statistics](#)
- [Displaying DNS Rule Proximity Statistics](#)
- [Displaying DNS Rule Statistics](#)
- [Displaying Source Address Statistics](#)
- [Displaying Source Address List Statistics](#)
- [Displaying DNS Rule Sticky Statistics](#)

Displaying Answer Statistics

You display the accumulated hit count for each configured answer that responds to content queries by using the **show statistics dns answer** command. The statistics also include the per second average hit count calculated during the last-minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is as follows:

```
show statistics dns answer {list | answer_name}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all answers configured for the GSS.
- *answer_name*—Name of the answer that you want to display statistics.

[Table 13-1](#) describes the fields in the **show statistics dns answer** command output.

Table 13-1 *Field Descriptions for show statistics dns answer Command*

Field	Description
Answer	Name of the answer. Depending on the type of answer, the GSS displays the following: <ul style="list-style-type: none"> • VIP address of the answer (VIP-type answer) • Interface or circuit address (CRA-type answer) • IP address of the name server (Name Server-type answer)
Type	Resources to which the GSS resolves DNS requests. The answer types include VIP, CRA, or Name Server (NS).
Total Hits	Total number of hits for the configured answer since the GSS was last started or statistics cleared.
1-Min	Averaged per second hit count for the answer, calculated during the last minute.
5-Min	Averaged per second hit count for the answer, calculated during the last 5-minute interval.

Table 13-1 *Field Descriptions for show statistics dns answer Command (continued)*

Field	Description
30-Min	Averaged per second hit count for the answer, calculated during the last 30-minute interval.
4-Hr	Averaged per second hit count for the answer, calculated during the last 4-hour interval.

Displaying Answer Group Statistics

You display the total hit count for each configured answer group and the answers contained in the answer group by using the **show statistics dns answer-group** command.

The syntax for the command is as follows:

```
show statistics dns answer-group {list | group_name [verbose]}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all answer groups configured for the GSS.
- *group_name*—Name of the answer group that you want to display statistics.
- **verbose**—Allows you to display detailed statistics for each answer that makes up an answer group.

Table 13-2 describes the fields in the `show statistics dns answer-group verbose` command output.

Table 13-2 *Field Descriptions for show statistics dns answer-group verbose Command*

Field	Description
Total Hit Count	Accumulated hit count for the configured answer group since the GSS was last started.
Answer	Name of each answer in the answer group. Depending on the type of answer, the GSS displays the following: <ul style="list-style-type: none">• VIP address of the answer (VIP-type answer)• Interface or circuit address (CRA-type answer)• IP address of the name server (Name Server-type answer)
Hit Count	Number of times that the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.
Status	Indicates whether the answer is online (up) or offline (down).

Displaying Domain Statistics

You display the accumulated hit count for each configured host domain by using the **show statistics dns domain** command. The statistics also include the per-second average hit count calculated during the last minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is as follows:

```
show statistics dns domain {list | domain_name }
```

The keywords and arguments are as follows:

- **list**—Lists the names of all domains configured for the GSS.
- *domain_name*—Name of the domain that you want to display statistics.

[Table 13-3](#) describes the fields in the **show statistics dns domain** command output.

Table 13-3 *Field Descriptions for show statistics dns domain Command*

Field	Description
Domain	Name of the hosted domain.
Total Hits	Total number of hits for the specified hosted domain since the GSS was last started.
1-Min	Averaged per second hit count for the hosted domain, calculated during the last minute.
5-Min	Averaged per second hit count for the hosted domain, calculated during the last 5-minute interval.
30-Min	Averaged per second hit count for the hosted domain, calculated during the last 30-minute interval.
4-Hr	Averaged per second hit count for the hosted domain, calculated during the last 4-hour interval.

Displaying Domain List Statistics

You display the total accumulated hit count for each configured domain list by using the **show statistics dns domain-list** command.

The syntax for the command is as follows:

```
show statistics dns domain-list {list | domain_list_name [verbose]}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all domains configured for the GSS.
- *domain_list_name*—Name of the domain list that you want to display statistics.
- **verbose**—Allows you to display detailed statistics for each domain that makes up a domain list.

Table 13-4 describes the fields in the **show statistics dns domain-list verbose** command output.

Table 13-4 *Field Descriptions for show statistics dns domain-list verbose Command*

Field	Description
Total Hit Count	Accumulated hit count for the hosted domain since the GSS was last started or statistics cleared.
Domain Name	Name of the hosted domain in the domain list.
Hit Count	Number of times that the hosted domain has been selected or matched in the DNS rule when the GSS processes a DNS request.

Displaying Global Statistics

You display general DNS statistics for the GSS device in use by using the **show statistics dns global** command.

The syntax for the command is as follows:

```
show statistics dns global
```

Table 13-5 describes the fields in the **show statistics dns global** command output.

Table 13-5 *Field Descriptions for show statistics dns global Command*

Field	Description
DnsQueriesRcvd	Total number of DNS queries received by the GSS from a requesting client D-proxy.
DnsHostAddrQueriesRcvd	Total number of host address queries received by the GSS from a requesting client D-proxy.
DnsResponsesSent	Total number of DNS responses sent by the GSS to a requesting client D-proxy.
DnsResponsesNoError	Total number of DNS responses sent by the GSS to a requesting client D-proxy without an error.
DnsResponsesErrors	Total number of DNS responses sent by the GSS to a requesting client D-proxy with an error.
DnsServfailRCode	DNS server failure return code.
DnsNxdomainRCode	DNS NX domain return code.
DnsNotimpRCode	DNS not implemented return code.
DnsRefusedRCode	DNS refused return code.
DnsQueriesUnmatched	Total number of unmatched DNS queries received by the GSS from a requesting client D-proxy.
DnsDrops	Total number of DNS queries dropped by the GSS.
DnsNSFWDSent	Total number of queries that do not match domains on any GSS domain lists and have been forwarded by the GSS to an external DNS name server for resolution.

Table 13-5 *Field Descriptions for show statistics dns global Command (continued)*

Field	Description
DnsBoomServReqSent	Total number of requests sent by the boomerang server in the GSS to initiate a DNS race.
DnsNSFWDResponsesRcvd	Total number of queries that have been forwarded to the GSS to an external DNS name server for resolution.
DnsProxLkupReqSent	Total number of proximity lookup requests sent by the selector to the proximity subsystem.
DnsProxLkupRespRecd	Total number of proximity lookup requests received by the selector from the proximity subsystem.
DnsReqRatePerSecondCur	Current request rate per second that requests are made to the GSS to perform a DNS resolution.
DnsReqRatePerSecondPeak	Peak request rate per second that requests are made to the GSS to perform a DNS resolution.
DnsStickyLkupReqSent	Total number of sticky lookup requests sent by the selector to the sticky subsystem.
DnsStickyAddReqSent	Total number of requests for IP addresses sent by the selector to the sticky subsystem.
DnsStickyHit	Total number of successful sticky answer matches for the DNS rule.
DnsStickyMiss	Total number of times that the GSS was unable to provide the sticky answer for the DNS rule.
DnsSrcPortErrorUdp	Total number of UDP errors that occurred on the DNS source port.
DnsSrcPortErrorTcp	Total number of TCP errors that occurred on the DNS source port.
DnsPollSocketError	Total number of socket connection errors.

Displaying DNS Rule Proximity Statistics

You display all proximity lookups by DNS rule name by using **show statistics dns proximity rule** command.



Note

To clear proximity statistics related to the DNS server component of the GSS, use the **clear statistics dns** command. See the [“Clearing GSS Global Server Load-Balancing Statistics”](#) section for details.

The syntax for the command is as follows:

```
show statistics dns proximity rule
```

[Table 13-6](#) describes the fields in the **show statistics dns proximity rule** command output.

Table 13-6 *Field Descriptions for show statistics dns proximity rule Command*

Field	Description
Rule	Name of the matched DNS rule.
Proximity Hit Count	Number of DNS requests that match the DNS rule.
Proximity Success Count	Number of DNS responses successfully returned with a proximate answer for the DNS rule.

Displaying DNS Rule Statistics

You display the total hit count and success count for each configured DNS rule by using the **show statistics dns rule** command.

The syntax for the command is as follows:

```
show statistics dns rule {list | rule_name}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all DNS rules configured for the GSS.
- *rule_name*—Name of the DNS rule that you want to display statistics.

Table 13-7 describes the fields in the **show statistics dns rule** command output.

Table 13-7 Field Descriptions for show statistics dns rule Command

Field	Description
Total Hit Count	Accumulated hit count for the configured DNS rule since the GSS was last started.
Total Success Count	Accumulated number of successful answer matches for the DNS rule.
Clause	Number of the balance clause in the DNS rule.
Hit Count	Number of times that the DNS rule processed a DNS request.
Success Count	Number of successful answer matches for the DNS rule.
Id	Internal ID number of the answer in the DNS rule.
Address	Name of the answer. Depending on the type of answer, the GSS displays the following: <ul style="list-style-type: none">• VIP address of the answer (VIP-type answer)• Interface or circuit address (CRA-type answer)• IP address of the name server (Name Server-type answer)
Hit Count	Number of times that the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.

Displaying Source Address Statistics

You display the accumulated hit count for each configured source address by using the **show statistics dns source-address** command. The statistics also includes the per-second average hit count calculated during the last-minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is as follows:

```
show statistics dns source-address {list | sa_name}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all source addresses configured for the GSS.
- *sa_name*—Name of the source address that you want to display statistics.

[Table 13-8](#) describes the fields in the **show statistics dns source-address** command output.

Table 13-8 Field Descriptions for *show statistics dns source-address* Command

Field	Description
Src Address	IP address or CIDR address block of the client DNS proxy.
Total Hits	Total number of hits for the source address since the GSS was last started or statistics cleared.
1-Min	Averaged per second hit count for the source address, calculated during the last minute.
5-Min	Averaged per second hit count for the source address, calculated during the last 5-minute interval.
30-Min	Averaged per second hit count for the source address, calculated during the last 30-minute interval.
4-Hr	Averaged per second hit count for the source address, calculated during the last 4-hour interval.

Displaying Source Address List Statistics

You display the total hit count for each configured source address list by using the **show statistics dns source-address-list** command. The statistics also include the last minute average, 5-minute average, 30-minute average, and 4-hour average of the hit counts.

The syntax for the command is as follows:

```
show statistics dns source-address-list {list | sa_list_name [verbose]}
```

The keywords and arguments are as follows:

- **list**—Lists the names of all source addresses.
- *sa_list_name*—Name of the source address list that you want to display statistics.
- **verbose**—Allows you to display detailed statistics for each name in the source address list.

[Table 13-9](#) describes the fields in the **show statistics dns source-address-list** command output.

Table 13-9 *Field Descriptions for show statistics dns source-address-list verbose Command*

Field	Description
Total Hit Count	Accumulated hit count for the configured source address list since the GSS was last started or statistics cleared.
Source Address	IP address or CIDR address block of the client DNS proxy.
Hit Count	Number of times that the source address has been selected or matched in the DNS rule when the GSS processes a DNS request.

Displaying DNS Rule Sticky Statistics

You display all DNS sticky lookups by DNS rule name by using the **show statistics dns sticky rule** command



Note

You clear sticky statistics related to the DNS server component of the GSS by using the **clear statistics dns** command. See the [“Clearing GSS Global Server Load-Balancing Statistics”](#) section for details.

The syntax for the command is as follows:

```
show statistics dns sticky rule
```

[Table 13-10](#) describes the fields in the **show statistics dns sticky rule** command output.

Table 13-10 Field Descriptions for show statistics dns sticky rule Command

Field	Description
Rule	Name of the matched DNS rule.
Sticky Hit Count	Total number of lookups in the sticky database for the DNS rule.
Sticky Success Count	Total number of successful sticky answer matches for the DNS rule.

Displaying the Status of the DRP Agent on a GSS

You display statistics on the Director Response Protocol (DRP) agent by using the **show statistics drpagent** command.



Note

You clear statistics related to the DRP agent component of the GSS by using the **clear statistics drpagent** command. See the “[Clearing GSS Global Server Load-Balancing Statistics](#)” section for details.

The syntax for the command is as follows:

```
show statistics drpagent
```

[Table 13-11](#) describes the fields in the **show statistics drpagent** command output.

Table 13-11 Field Descriptions for show statistics drpagent Command

Field	Description
DRP agent enabled/disabled	DRP agent status, enabled or disabled.
director requests	Number of director requests.
successful measured lookups	Number of successful DRP measure requests received by the DRP agent from all of the GSSs.
packet failures returned	Number of packet failures returned.
successful echos	Number of successful DRP echo requests (DRP keepalives) received by the DRP agent from all of the GSSs.
path-rtt probe source port	Source port of the path probe packets from the DRP agent.
path-rtt probe destination port	Destination port of the path probe packets from the DRP agent.
tcp-rtt probe source port	Source port of the TCP probe packets from the DRP agent.
tcp-rtt probe destination port	Destination port of the TCP probe packets from the DRP agent.

Displaying DDoS Statistics on a GSS

This section describes the procedures you need to follow to display DDoS statistics from the CLI. It contains the following topics:

- [Displaying DDoS Attack Statistics](#)
- [Displaying DDoS Anti-Spoofing Statistics](#)
- [Displaying DDoS Failed DNS Queries](#)
- [Displaying DDoS Rate-Limit Values](#)
- [Displaying DDoS Running Configuration](#)
- [Displaying DDoS Statistics](#)
- [Displaying DDoS Status](#)

Displaying DDoS Attack Statistics

You display the DNS attacks detected by the GSS by using the **show ddos attacks** (from privileged EXEC mode) or **show attacks** (from ddos configuration mode) commands.

**Note**

Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is as follows:

```
show [ddos] attacks
```

[Table 13-12](#) describes the fields in the **show [ddos] attacks** command output.

Table 13-12 Field Descriptions for show [ddos] attacks Command

Field	Description
Total Attacks	Total number of DNS attacks detected by the GSS.
Reflection attack	Attack in which the IP address of the victim (that is, the GSS) is spoofed and multiple DNS requests are sent to a DNS server or multiple DNS servers posing as the victim.
Malformed DNS packet attacks	Attack in which the GSS is flooded with malformed DNS packets.
Failed Global Domain attacks	Failed domain counter provides a total for DNS queries that failed to match the global domain name.
Global Rate-limit exceeded attacks	Attack in which the maximum number of DNS requests the GSS receives from the D-proxy per second exceeds the global limit.

For example:

```
gssm1.example.com(config-ddos)# show attacks

Total Attacks                               :0
  Reflection attack                          :0
  Malformed DNS packet attacks               :0
  Failed Global Domain attacks               :0
  Global Rate-limit exceeded attacks:0
```

Displaying DDoS Anti-Spoofing Statistics

You display the spoofed and trusted D-proxies on the GSS by using the **show ddos dproxy** (from privileged EXEC mode) or **show dproxy** (from ddos configuration mode) commands.



Note

Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is as follows:

```
show [ddos] dproxy [ipaddress | spoofed | trusted]
```

The keywords and arguments are as follows:

- *ipaddress*—D-proxy IP address.
- **spoofed**—Shows the spoofed D-proxies.
- **trusted**—Shows the trusted D-proxies.

Table 13-13 describes the fields in the **show ddos dproxy** command output.

Table 13-13 Field Descriptions for show [ddos] d-proxy Command

Field	Description
Dproxy Address	IP address of the D-proxy.
Spoofed/Nonspoofed	Spoofed or non-spoofed D-proxy.
Drops	Number of dropped packets due to anti-spoofing failure.

For example:

```
gssm1.example.com# show ddos dproxy 16.1.1.11

      DPROXY ADDRESS      SPOOFED/NONSPOOFEDDROPS
      -----            -
      16.1.1.11           Spoofed                   3
```

Displaying DDoS Failed DNS Queries

You use the **show ddos failed-dns** (from privileged EXEC mode) or **show failed-dns** (from ddos configuration mode) commands to show the following:

- the last *x* number of domain names that caused failed DNS queries at the GSS
- the number of failed DNS queries per D-proxy

Failed DNS queries refer to DNS queries for a domain not configured on the GSS.



Note

Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is as follows:

```
show [ddos] failed-dns [failed-domains | global-domain-rules | gslb-rules]
```

The keywords and arguments are as follows:

- **failed-domains**—Shows the failed domain names due to a GSLB-rule mismatch.



Note

Even if DDoS is disabled, you can use this option to list the failed domain names due to the GSLB-rule mismatch. The list is updated even if DDoS is disabled.

- **global-domain-rules**—Shows the number of failures due to a global domain mismatch.
- **gslb-rules**—Shows the number of failures due to a GSLB-rule mismatch.

[Table 13-14](#) describes the fields in the `show [ddos] failed-dns` command output.

Table 13-14 Field Description for show [ddos] failed-dns Command

Field	Description
Global domain check drops	Number of dropped packets as a result of a global domain name check.
Dproxy Address	IP address of the D-proxy.
Number of Failed DNS queries	Number of failed DNS queries as a result of a GSLB-rule check.

For example, enter:

```
gssm1.example.com# show ddos failed-dns failed-domains
www.test.com
www.test.com
www.example.com
```

```
gssm1.example.com# show ddos failed-dns global-domain-rules
Global domain check drops:4
```

```
gssm1.example.com# show ddos failed-dns gslb-rules
```

```

DPROXY ADDRESS      NUMBER OF FAILED DNS QUERIES
-----
16.1.1.14           0
16.1.1.13           0
16.1.1.11           0
16.1.1.12           0

```

Displaying DDoS Rate-Limit Values

You display the rate limits per D-proxy and the number of packets dropped per source by using the **show ddos rate-limit** (from privileged EXEC mode) or **show rate-limit** (from ddos configuration mode) commands.

The syntax for the command is as follows:

```
show [ddos] rate-limit [ipaddress | global | unknown]
```

The keywords and arguments are as follows:

- *ipaddress*—IP address of the D-proxy.
- **global**—Specifies the global rate limit on the GSS.
- **unknown**—Specifies the unknown D-proxy rate limit on the GSS.

[Table 13-15](#) describes the fields in the **show [ddos] rate-limit** command output.

Table 13-15 Field Descriptions for show [ddos] rate-limit Command

Field	Description
Dproxy Address	IP address of the D-proxy.
Rate-limit	Maximum number of DNS requests that the GSS can receive from a D-proxy per second.
Applied Rate Limit	This value is based on the following: rate-limit * scaling factor/100
Drops	Number of packets dropped because of the rate-limit.

For example:

```

gssm1.example.com# show ddos rate-limit 16.1.1.11

Dproxy Address      Rate-limit Applied Rate Limit      Drops
-----

```

```
16.1.1.11      0      12000      0
```

Displaying DDoS Running Configuration

You display the contents of the DDoS running configuration file by using the **show ddos-config** (from privileged EXEC or ddos configuration mode) command.

The syntax for the command is as follows:

```
show ddos-config
```

Table 13-16 describes the fields in the **show ddos-config** command output.

Table 13-16 Field Descriptions for show ddos-config Command

Field	Description
enable	DDoS detection and mitigation module status, enabled or disabled.
rate-limit global	Global rate limit configured on the GSS.
tolerance factor	Helps determine the rate limit.
peacetime database	Peacetime database identifier.
global domain	Global domain name identifier.
dproxy trusted	D-proxy added or deleted from a trusted D-proxy database.
mitigation-rule response enable	Enables mitigation rules for the following DNS responses: <ul style="list-style-type: none"> • Packets are dropped with a source port other than 53 and QR bit of 1 (response) when responses come from a source port other than 53. • Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.
mitigation-rule request enable	Enables mitigation rules for DNS requests in which packets are dropped with a source port equal to 53, but less than 1024, and a QR bit of 0 (request).

For example, enter:

```
gssm1.example.com# show ddos-config
ddos
  enable
  rate-limit global 10000
  tolerance-factor dproxy 2
  peacetime database abc
  global domain www.level1.com
  dproxy trusted 16.1.1.13
  dproxy trusted 16.1.1.14
  rate-limit 16.1.1.12 40
  rate-limit 16.1.1.11 40
  mitigation-rule response enable
  mitigation-rule request enable
```

Displaying DDoS Statistics

You display DDoS statistics by using the **show statistics ddos** (from privileged EXEC mode), or **show statistics** (from ddos configuration mode) commands.



Note

You clear statistics related to the DDoS detection and mitigation component of the GSS by using the **clear statistics ddos** command. See the [“Clearing GSS Global Server Load-Balancing Statistics”](#) section for details.

The syntax for the command is as follows:

```
show statistics [ddos] [attacks | global]
```

The keywords and arguments are as follows:

- **attacks**—Displays attack statistics.
- **global**—Displays global statistics.

[Table 13-17](#) describes the fields in the **show statistics ddos attacks** command output.

Table 13-17 Field Descriptions for show statistics ddos attacks Command

Field	Description
Total Attacks	Total number of DDoS attacks on the GSS.
Reflection attacks	Attack in which the IP address of the victim (that is, the GSS) is spoofed and multiple DNS requests are sent to a DNS server or multiple DNS servers posing as the victim.
Malformed DNS packet attacks	Attack in which the GSS is flooded with malformed DNS packets.
Failed Global Domain attacks	An attack in which the GSS is flooded with failed global domain attacks.
Global Rate-limit exceeded attacks	Attack in which the global rate-limit threshold has been exceeded.

For example, enter:

```
gssm1.example.com# show statistics ddos attacks
```

```

Total Attacks                               :0
  Reflection attack                          :0
  Malformed DNS packet attacks               :0
  Failed Global Domain attacks               :0
  Global Rate-limit exceeded attacks:0

```

[Table 13-18](#) describes the fields in the **show statistics ddos global** command output.

Table 13-18 Field Descriptions for show statistics ddos global Command

Field	Description
Total packets received	Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.
Total packets dropped	Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.

Table 13-18 Field Descriptions for show statistics ddos global Command (continued)

Field	Description
Total Anti-spoofing triggered	Total number of packets that triggered the GSS anti-spoofing mechanism.
Total Validated DNS requests	Total number of packets successfully identified as part of an anti-spoofing attack.
Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation rate-limiting functions as part of an attack and dropped. The rate limit is the maximum number of DNS requests that the GSS can receive from the D-proxy per second.
Global Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.
Unknown dproxies drops	An D-proxy that has not been classified as spoofed or non-spoofed by the DDoS protection and mitigation function is unknown. The DDoS function starts anti-spoofing for an unknown D-proxy. If the number of packets from unknown D-Proxies exceeds the specified rate limit, the unknown drops start.
Spoofed packet drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an attack and dropped.
Malformed packet drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a malformed packet and dropped.
Mitigation rules drops	Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.
Global domain name drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.
Ongoing anti-spoofing drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.

For example, enter:

```
gssm1.example.com# show statistics ddos global
Total packets received      :6
Total packets dropped       :2

Total Anti-Spoofing triggered:0
Total Validated DNS requests :0

Dropped Packets Statistics:
-----
Rate limit drops            :0
Global Rate limit drops    :0
Unknown dproxies drops     :0
Spoofed packet drops       :2
Malformed packet drops     :0
Mitigation rule drops      :0
Global domain drops        :0
Ongoing anti-spoofing drops :0
```

Displaying DDoS Status

You display DDoS status by using the **show ddos status** (from privileged EXEC mode) or **show status** (from ddos configuration mode) commands.

The syntax for the command is as follows:

```
show [ddos] status
```

Table 13-19 describes the fields in the **show ddos status** command output.

Table 13-19 Field Description for show [ddos] status Command

Field	Description
DDoS Status	Status of the DDoS detection and mitigation module in the GSS, either enabled or disabled.

For example, enter:

```
gss1.yourdomain.com# show ddos status
DDoS Status: Disabled
```

Displaying the Status of Keepalives on a GSS

The keepalive engine on each GSS device monitors the current online status of the configured keepalives managed by the GSS. You can display statistics for all keepalive types on your network, or limit statistics to a specific keepalive type, such as CRA, HTTP HEAD, ICMP, KAL-AP, name server, or TCP.

Use the **show statistics keepalive** command option to display statistics about the health of your GSS keepalives globally or by keepalive type.

This section contains the following topics:

- [Displaying CRA Keepalive Statistics](#)
- [Displaying Global Keepalive Statistics](#)
- [Displaying HTTP HEAD Keepalive Statistics](#)
- [Displaying ICMP Keepalive Statistics](#)
- [Displaying KAL-AP Keepalive Statistics](#)
- [Displaying Scripted Keepalive Statistics](#)
- [Displaying Name Server Keepalive Statistics](#)
- [Displaying TCP Keepalive Statistics](#)
- [Displaying Keepalive Answer Type Statistics](#)

Displaying CRA Keepalive Statistics

You display statistics for configured content routing agent (CRA) keepalive types managed by the GSS and used with boomerang-type answers by using the **show statistics keepalive cra** command.

The syntax for the command is as follows:

```
show statistics keepalive cra { ip_address | all | list }
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured CRA-type keepalives.
- **list**—Lists all available IP addresses.

Table 13-20 describes the fields in the **show statistics keepalive cra all** command output.

Table 13-20 Field Descriptions for show statistics keepalive cra all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	Name assigned to the answer.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
One Way Delay	One-way delay time, in milliseconds, used by the GSS to calculate a static round-trip time (RTT), with the one-way delay constituting one-half of the round-trip time that is used for all DNS races involving this answer.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying Global Keepalive Statistics

You display all keepalive statistics managed by the GSS device by using the **show statistics keepalive global** command.

The syntax for the command is as follows:

```
show statistics keepalive global
```

Table 13-21 describes the fields in the **show statistics keepalive global** command output.

Table 13-21 Field Descriptions for show statistics keepalive global Command

Field	Description
ICMP Probe Success Count	Number of ICMP queries sent to the answer that resulted in a successful response.
ICMP Probe Failure Count	Number of ICMP queries sent to the answer that resulted in a failure.
ICMP 'echo request' packets sent	Number of ICMP echo request messages sent to the answer.
ICMP 'echo reply' packets received	Number of ICMP echo reply messages received by the GSS from the answer.
Configured ICMP Probe Count	Number of configured ICMP probes sent to the answer.
ONLINE ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Online state for the keepalive.
OFFLINE ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Offline state for the keepalive.
SUSPENDED ICMP Probe Count	Number of ICMP probes sent to the answer that returned a Suspended state for the keepalive.
INIT ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Init state for the keepalive.
DNS Probe Success Count	Number of DNS request probes sent by the GSS that resulted in a successful response.

Table 13-21 Field Descriptions for *show statistics keepalive global* Command (continued)

Field	Description
DNS Probe Failure Count	Number of DNS request probes sent by the GSS that resulted in a failure.
DNS packets sent	Number of DNS request packets sent by the GSS.
DNS packets received	Number of DNS request packets received by the GSS.
Configured DNS Probe Count	Number of DNS request probes sent by the GSS.
ONLINE DNS Probe Count	Number of DNS request probes sent that returned an Online state for the keepalive.
OFFLINE DNS Probe Count	Number of DNS request probes that returned an Offline state for the keepalive.
SUSPENDED DNS Probe Count	Number of DNS request probes sent that returned a Suspended state for the keepalive.
INIT DNS Probe Count	Number of DNS request probes sent that returned an Init state for the keepalive.
KAL-AP Probe Success Count	Number of KAL-AP queries sent to the answer that resulted in a successful response.
KAL-AP Probe Failure Count	Number of KAL-AP queries sent to the answer that resulted in a failure.
KAL-AP packets sent	Number of KAL-AP packets sent to the answer.
KAL-AP packets received	Number of KAL-AP packets received by the GSS from the answer.
Configured KAL-AP Probe Count	Number of configured KAL-AP probes sent to the answer.
ONLINE KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Online state for the keepalive.
OFFLINE KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive.

Table 13-21 Field Descriptions for *show statistics keepalive global* Command (continued)

Field	Description
SUSPENDED KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive.
INIT KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive.
CRA Probe Success Count	Number of CRA queries sent to the answer that resulted in a successful response.
CRA Probe Failure Count	Number of CRA queries sent to the answer that resulted in a failure.
CRA packets sent	Number of CRA packets sent to the answer.
CRA packets received	Number of CRA packets received by the GSS from the answer.
Configured CRA Probe Count	Number of configured CRA probes sent to the answer.
ONLINE CRA Probe Count	Number of CRA probes sent to the answer that returned an Online state for the keepalive.
OFFLINE CRA Probe Count	Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive.
SUSPENDED CRA Probe Count	Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive.
INIT CRA Probe Count	Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive.
HTTP-HEAD Probe Success Count	Number of HTTP-HEAD queries sent to the answer that resulted in a successful response.
HTTP-HEAD Probe Failure Count	Number of HTTP-HEAD queries sent to the answer that resulted in a failure.
HTTP-HEAD packets sent	Number of HTTP-HEAD packets sent to the answer.
HTTP-HEAD packets received	Number of HTTP-HEAD packets received by the GSS from the answer.

Table 13-21 Field Descriptions for *show statistics keepalive global* Command (continued)

Field	Description
Configured HTTP-HEAD Probe Count	Number of configured HTTP-HEAD probes sent to the answer.
ONLINE HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Online state for the keepalive.
OFFLINE HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Offline state for the keepalive.
SUSPENDED HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned a Suspended state for the keepalive.
INIT HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Init state for the keepalive.
TCP Probe Success Count	Number of TCP queries sent to the answer that resulted in a successful response.
TCP Probe Failure Count	Number of TCP queries sent to the answer that resulted in a failure.
TCP packets sent	Number of TCP packets sent to the answer.
TCP packets received	Number of TCP packets received by the GSS from the answer.
Configured TCP Probe Count	Number of configured TCP probes sent to the answer.
ONLINE TCP Probe Count	Number of TCP probes sent to the answer that returned an Online state for the keepalive.
OFFLINE TCP Probe Count	Number of TCP probes sent to the answer that returned an Offline state for the keepalive.
SUSPENDED TCP Probe Count	Number of TCP probes sent to the answer that returned a Suspended state for the keepalive.

Table 13-21 Field Descriptions for *show statistics keepalive global Command (continued)*

Field	Description
INIT TCP Probe Count	Number of TCP probes sent to the answer that returned an Init state for the keepalive.
Total Configured Probe Count	Total number of configured keepalive probes.

Displaying HTTP HEAD Keepalive Statistics

You display statistics for configured HTTP HEAD keepalive types managed by the GSS and used with VIP-type answers by using the **show statistics keepalive http-head** command.

The syntax for the command is as follows:

```
show statistics keepalive http-head {ip_address | all | list}
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured HTTP HEAD-type keepalives.
- **list**—Lists all available IP addresses.

[Table 13-22](#) describes the fields in the **show statistics keepalive http-head all** command output.

Table 13-22 Field Descriptions for *show statistics keepalive http-head all Command*

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.

Table 13-22 Field Descriptions for `show statistics keepalive http-head all` Command (continued)

Field	Description
Keepalive Type	Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Destination Port	Port on the remote device receiving the HTTP HEAD-type keepalive request from the GSS.
HTTP Path	Default path that is relative to the server website being queried in the HTTP HEAD request.
Host Tag	Domain name that is sent to the VIP as part of the HTTP HEAD query in the Host tag field of the shared keepalive configuration.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying ICMP Keepalive Statistics

You display statistics for configured ICMP keepalive types managed by the GSS and used with VIP-type answers by using the `show statistics keepalive icmp` command.

The syntax for the command is as follows:

```
show statistics keepalive icmp { ip_address | all | list }
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured ICMP-type keepalives.
- **list**—Lists all available IP addresses.

Table 13-23 describes the fields in the **show statistics keepalive icmp all** command output.

Table 13-23 Field Descriptions for show statistics keepalive icmp all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying KAL-AP Keepalive Statistics

You display statistics for configured KAL-AP keepalive types managed by the GSS and used with VIP-type answers by using the **show statistics keepalive kalap** command.

The syntax for the command is as follows:

```
show statistics keepalive kalap { ip_address | all | list }
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured KAL-AP-type keepalives.
- **list**—Lists all available IP addresses.

Table 13-24 describes the fields in the **show statistics keepalive kalap all** command output.

Table 13-24 Field Descriptions for show statistics keepalive kalap all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	The Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Tag	Alphanumeric tag associated with the VIP in the KAL-AP request.
Primary Circuit	Primary (master) IP address.
Secondary Circuit	Secondary (backup) IP address.
Load	Load threshold value used to determine whether an answer is available, regardless of the balance method used.

Table 13-24 Field Descriptions for *show statistics keepalive kalap all* Command (continued)

Field	Description
Circuit Transitions	Number of times that the circuit changed state.
VIP Failovers	Number of times the VIP switched to or from the primary DNS server and the secondary DNS server.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying Scripted Keepalive Statistics

You display statistics for configured Scripted keepalive types managed by the GSS and used with VIP-type answers by using the **show statistics keepalive scripted-kal** command.

The syntax for the command is as follows:

```
show statistics keepalive scripted-kal {name | all | list}
```

The keywords and arguments are as follows:

- *name*—Keepalive name for which you wish to display keepalive statistics.
- **all**—Displays all configured Scripted keepalives.
- **list**—Lists all available IP addresses.

Table 13-25 describes the fields in the `show statistics keepalive scripted-kal all` command output.

Table 13-25 Field Descriptions for `show statistics keepalive scripted-kal all` Command

Field	Description
Kal Name	Name of the applicable keepalive.
SLB Address	IP address of the SLB.
OID	SNMP request sent for this OID. There are two types of OIDs: scalar and vector or table. For a scalar-type OID, the filter is not necessary, while for a vector-type, it is a requirement. When you query for the vector OID, you get all the information in the table that describes all of the VIPs configured at the target device. In this data, the load information for some VIPs configured at the GSS is the only information of real value, however.
VIP Address	Address of the VIP.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Load	Load threshold value used to determine whether an answer is available, regardless of the balance method used.
Community Name	SNMP community name defined at the target device.

Table 13-25 Field Descriptions for show statistics keepalive scripted-kal all Command (continued)

Field	Description
Filter	<p>Required entry when fetching load information for some VIPs configured at the GSS. For example, the following CLI commands shows how the filter is specified in the form of an address-filter and load filter:</p> <pre>(config-gslb)#shared-keepalive scripted-kal kal-name CSS1-VIP-STATUS-TABLE snmp-mib-not-indexed-by-vip slb-address 1.1.1.1 oid 1.3.6.1.4.1.9.9.161.1.4 community public filter 9.9.161.1.4.1.1.4,9.9.161.1.4.1.1.17</pre> <pre>(config-gslb)#shared-keepalive scripted-kal kal-name CSS1-VIP-STATUS-TABLE snmp-mib-indexed-by-vip slb-address 1.1.1.1 oid 1.3.6.1.4.1.9.9.161.1.3.1 community public filter 9.9.161.1.3.1.1.4</pre>
Scripted Kal Type	Type of Scripted keepalive. The potential types are cisco-slb, f5-slb, snmp-mib-indexed-by-vip, snmp-mib-not-indexed-by-vip, and snmp-scalar.
No. of Execution	Number of times that the script is executed.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
VIP GID	VIP Global ID number used by the GSS.
LID	Local ID number used by the GSS.
Keepalive GID	Global ID number of the keepalive.

Displaying Name Server Keepalive Statistics

You display statistics for configured name server (NS) keepalive types managed by the GSS and used with name server type answers by using the **show statistics keepalive ns** command.

The syntax for the command is as follows:

```
show statistics keepalive ns { ip_address | all | list }
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured name server-type keepalives.
- **list**—Lists all available IP addresses.

Table 13-26 describes the fields in the **show statistics keepalive ns all** command output.

Table 13-26 Field Descriptions for show statistics keepalive ns all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Domain	Globally defined domain name that the GSS queries when utilizing the NS keepalive.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.

Table 13-26 Field Descriptions for *show statistics keepalive ns all* Command (continued)

Field	Description
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying TCP Keepalive Statistics

You display statistics for configured TCP keepalive types managed by the GSS and used with VIP-type answers by using the **show statistics keepalive tcp** command.

The syntax for the command is as follows:

```
show statistics keepalive tcp { ip_address | all | list }
```

The keywords and arguments are as follows:

- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured TCP-type keepalives.
- **list**—Lists all available IP addresses.

[Table 13-27](#) describes the fields in the **show statistics keepalive tcp all** command output.

Table 13-27 Field Descriptions for *show statistics keepalive tcp all* Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.

Table 13-27 Field Descriptions for `show statistics keepalive tcp all` Command (continued)

Field	Description
Keepalive Type	Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Destination Port	Port on the remote device receiving the TCP keepalive request.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying Keepalive Answer Type Statistics

You display statistics for configured keepalive answers of type CRA, NS, and VIP, managed by the GSS by using the **show statistics keepalive answer type** command. The list that appears also includes statistics for multiple keepalives if assigned for a single VIP answer.

The syntax for the command is as follows:

```
show statistics keepalive answer type {cra | ns | vip {ip_address | all | list}}
```

The keywords and arguments are as follows:

- **cra**—Specifies the CRA keepalive type.
- **ns**—Specifies the NS keepalive type.
- **vip**—Specifies the VIP keepalive type.
- *ip_address*—IP address to display keepalive statistics.
- **all**—Displays all configured TCP-type keepalives.
- **list**—Lists all available IP addresses.

[Table 13-28](#) describes the fields in the **show statistics keepalive answer type** command output.

Table 13-28 Field Descriptions for show statistics keepalive answer type Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
GID	Global ID number used by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	The keepalive type (ICMP, TCP, HTTP HEAD, or KAL-AP) and the Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Destination Port	Port on the remote device receiving the keepalive request.
Termination method	The method that the GSS used to initiate closing of a connection (graceful or reset).
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.

Table 13-28 Field Descriptions for `show statistics keepalive answer type` Command (continued)

Field	Description
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.

Displaying Network Proximity Statistics on a GSS

The proximity component displays statistics about the network proximity of your GSS device. Network proximity statistics include information about the proximity database on the GSS device, individual zones, probing requests, and RTT coverage.

This section contains the following topics:

- [Displaying DNS Rule Proximity Statistics](#)
- [Displaying Proximity Database Statistics](#)
- [Displaying Proximity Group Statistics](#)
- [Displaying Proximity Lookup Statistics](#)
- [Displaying Proximity Probe Transfer Statistics](#)
- [Displaying Proximity Status](#)
- [Displaying Proximity Group Configuration](#)
- [Displaying Proximity Database Status](#)

Displaying DNS Rule Proximity Statistics

You display all proximity lookups by DNS rule name by using the **show statistics dns proximity rule** command.

The syntax for the command is as follows:

```
show statistics dns proximity rule
```

Table 13-29 describes the fields in the **show statistics dns proximity rule** command output.

Table 13-29 Field Descriptions for show statistics dns proximity rule Command

Field	Description
ProxRule	Name of the matched DNS rule.
Proximity Hit Count	Number of DNS requests that match the DNS rule.
Proximity Success Count	Number of DNS responses successfully returned with a proximate answer for the DNS rule.

Displaying Proximity Database Statistics

You display the overall statistics on the proximity database by using the **show statistics proximity database** command. Statistics include the number of entries currently in the proximity database, the number of entries dropped, and the rate of lookups.

The syntax for the command is as follows:

```
show statistics proximity database
```

Table 13-30 describes the fields in the **show statistics proximity database** command output.

Table 13-30 Field Descriptions for show statistics proximity database Command

Field	Description
Number of Entries in Use	Number of entries currently in the proximity database.
Number of Add Entries Dropped	Number of entry creation requests that the GSS dropped because the proximity database limit had been reached.
Max Number of Entries Used	Maximum number of entries used in the proximity database.
Max Number of Entries Allowed	Maximum number of entries that the proximity database can hold (500,000 entries).

Table 13-30 Field Descriptions for *show statistics proximity database* Command (continued)

Field	Description
Number of Database Dump Started	Number of times the GSS initiated a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps.
Number of Database Dump Completed	Number of times the GSS completed a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps.
Number of Database Dump Failed	Number of times the GSS failed to perform a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps.
Last Database Dump Started Time	The last time the GSS started a proximity database dump
Last Database Dump Failed Time	The last time the GSS failed to complete a proximity database dump.
Number of Database Cleanup Started	Number of times the GSS initiated a database cleanup to remove the least recently used entries from the proximity database.
Number of Database Cleanup Completed	Number of times the GSS completed a database cleanup to remove the least recently used entries from the proximity database.
Number of Database Cleanup Failed	Number of times the GSS failed to cleanup the least recently used entries from the proximity database.
Last Database Cleanup Started Time	The last time the GSS started the database cleanup process.
Last Database Cleanup Failed Time	The last time the GSS failed to complete the database cleanup process.

Displaying Proximity Group Statistics

You display a summary of statistics for all configured proximity groups by using the **show statistics proximity group-summary** command.

The syntax for the command is as follows:

```
show statistics proximity group-summary
```



Note

This command displays the proximity statistics to the console only if the number of proximity groups is less than 1000. If the number of proximity groups is more than 1000, an error message displays asking you to execute the **proximity statistics group-summary dump filename** command.

[Table 13-31](#) describes the fields in the **show statistics proximity group-summary** command output.

Table 13-31 Field Descriptions for show statistics proximity group-summary Command

Field	Description
Group Name	Unique alphanumeric name of the proximity group.
Target IP	Probe target IP address used by the proximity group, displayed in dotted-decimal notation.
Total Entries	Total number of D-proxy IP address and subnet mask pairs contained in the proximity group.
Total Hits	Accumulated hit count for all entries in the proximity group. Increments when a match occurs for any proximity group entry in the group

You display statistics for a specific proximity group by using the **show statistics proximity group-name** command.

The syntax for the command is as follows:

```
show statistics proximity group-name {groupname}
```

The *groupname* argument specifies the exact name of a proximity group in order to display all proximity database entries related to that group.

Table 13-32 describes the fields in the **show statistics proximity group-name** command output.

Table 13-32 Field Descriptions for show statistics proximity group-name Command

Field	Description
Group Name	Unique alphanumeric name of the proximity group.
Total Entries	Total number of D-proxy IP addresses or block of IP addresses included in the proximity group.
Target IP	Probe target IP address used by the proximity group, displayed in dotted-decimal notation.
Address	D-proxy IP address included in the proximity group.
Prefix	Subnet mask used to specify the block of IP addresses included in the proximity group, displayed as an integer (for example, 24 or 32).
Hit Counts	Increments when a match occurs for this proximity group entry.
Last Hit Time	Last time the hit count incremented due to an entry match.

Displaying Proximity Lookup Statistics

You display statistics about the proximity lookups that have occurred on this GSS by using the **show statistics proximity lookup** command.

The syntax for the command is as follows:

```
show statistics proximity lookup
```

Table 13-33 describes the fields in the **show statistics proximity lookup** command output.

Table 13-33 Field Descriptions for `show statistics proximity lookup` Command

Field	Description
Total lookup requests	Total number of proximity lookup requests made to the proximity database.
Database entry not found	Number of times the GSS was unable to locate a proximate answer in the database.
Partial RTT data returned	Number of times that only partial round-trip time (RTT) data was returned to the DNS service by the proximity subsystem.
Current lookup request rate	Current request rate per second that requests are made by the DNS service to perform a proximity lookup in the database.
Peak lookup request rate	Peak request rate per second that requests are made by the DNS service to perform a proximity lookup in the database.
Lookup failed due to database full	Number of times the GSS was unable to complete a proximity lookup because the database exceeded the maximum number of entries
Last database full happened	Last time the proximity database was full.

Displaying Proximity Probe Transfer Statistics

You display general probe success and failure counts by using the **show statistics proximity probes** command.

The syntax for the command is as follows:

```
show statistics proximity probes
```

[Table 13-34](#) describes the fields in the **show statistics proximity probes** command output.

Table 13-34 Field Descriptions for show statistics proximity probes Command

Field	Description
Authentication	Indicates whether the GSS performs DRP authentication when exchanging packets with the DRP agent in a probing device. States are Enabled and Disabled.
Echo Rx	Number of DRP echo responses received by the GSS from all configured probing devices.
Echo Tx	Number of DRP echo requests sent by the GSS to all configured probing devices.
Measure Rx	Number of DRP measured requests received by the GSS from all configured probing devices.
Measure Tx	Number of DRP measured requests sent by the GSS to all configured probing devices.
Pkts Rx	Total number of DRP packets received by the GSS from all configured probing devices.
Pkts Tx	Number of DRP packets sent by the GSS to all configured probing devices.

You display detailed statistics for the ICMP and TCP probes relative to all configured zones by using the **show statistics proximity probes detailed** command. This command also displays the operating status of the primary and secondary probing devices (ONLINE or OFFLINE).

The syntax for the command is as follows:

show statistics proximity probes detailed

[Table 13-35](#) describes the fields in the **show statistics proximity probes detailed** command output.

Table 13-35 Field Descriptions for show statistics proximity probes detailed Command

Field	Description
Zone ID	Numerical identifier of the proximity zone.
Zone Name	Name of the proximity zone.
Authentication	Indicates whether the GSS performs DRP authentication when exchanging packets with the DRP agent in a probing device.
Primary	IP address of the primary probing device servicing this zone and the status of the probing device (ONLINE or OFFLINE).
Secondary	IP address of the backup probing device servicing this zone and the status of the probing device (ONLINE or OFFLINE).
Echo Rx	Number of DRP echo responses received by the GSS from all configured probing devices.
Echo Tx	Number of DRP echo requests sent by the GSS to all configured probing devices.
Measure Rx	Number of DRP measured requests received by the GSS from all configured probing devices.
Measure Tx	Number of DRP measured requests sent by the GSS to all configured probing devices.
Pkts Rx	Total number of DRP packets received by the GSS from the probing device in the proximity zone.
Pkts Tx	Number of DRP packets sent by the GSS to the probing device in the proximity zone.
Pkts Rx Rate	Current received request rate per second.
Pkts Tx Rate	Current transmitted request rate per second.
Peak Rx Rate	Peak received request rate per second.
Peak Tx Rate	Peak transmitted request rate per second.

Displaying Proximity Status

You display general status information about the proximity subsystem by using the **show proximity** command.

The syntax for the command is as follows:

```
show proximity
```

Table 13-36 describes the fields in the **show proximity** command output.

Table 13-36 Field Descriptions for show proximity Command

Field	Description
Proximity subsystem status	Current operating status of the Proximity subsystem component.
Proximity database dump interval	Time period between automatic proximity database dumps performed by the GSS.
Proximity database age-out interval	Time period between checks by the GSS to verify when the user-configured entry inactivity timeout value elapses.

Displaying Proximity Group Configuration

You display a summary of all configured proximity groups by using the **show proximity group-summary** command.



Note

This command displays the configuration output to the console only if the number of proximity elements, or IP blocks, is less than 1000. (This value is not configurable). If the number of proximity elements is more than 1000, an error message displays asking you to execute the **proximity group-summary dump filename** command.

Table 13-37 describes the fields in the **show proximity group-summary** command output.

Table 13-37 Field Descriptions for show proximity group-summary Command

Field	Description
Name	Unique alphanumeric name of the proximity group.
Address Blocks	IP address block of the proximity group, specified in dotted-decimal notation.

You display the configuration of a specific proximity group by using the **show proximity group-name** command.

The syntax for the command is as follows:

```
show proximity group-name {groupname}
```

The *groupname* argument specifies the exact name of a proximity group in order to display all proximity entries related to that group.

[Table 13-38](#) describes the fields in the **show proximity group-name** command output.

Table 13-38 Field Descriptions for show proximity group-name Command

Field	Description
Name	Unique alphanumeric name of the proximity group.
Address Blocks	IP address block of the proximity group, specified in dotted-decimal notation.

Displaying Proximity Database Status

You display the proximity database entries by specifying one or more entry matching criteria by using the **show proximity database** command.

The syntax for this command is as follows:

```
show proximity database {all | assigned | group {name} | inactive minutes | ip {ip-address} netmask {netmask} | no-rtt | probed}
```

The keywords and arguments are:

- **all**—Displays all entries in the proximity database.
- **assigned**—Displays all static entries in the proximity database.

- **group name**—Displays all entries that belong to a named proximity group. Specify the exact name of a previously created proximity group.
- **inactive minutes**—Displays all dynamic entries that have been inactive for a specified time. Valid values are 0 to 43200 minutes.
- **ip ip-address netmask netmask**—Displays all proximity entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **no-rtt**—Displays all entries in the PDB that do not have valid RTT values.
- **probed**—Displays all dynamic entries in the PDB.

For example, to display entries related to the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gss1.example.com# show proximity database ip 192.168.8.0 255.255.255.0
```

Displaying DNS Sticky Statistics on a GSS

The sticky component displays statistics about the sticky operation of your GSS device. Sticky statistics include information about DNS sticky lookups by DNS rule name, entries in the sticky database on the GSS device, global sticky status and statistics, operating status and statistics on GSS peers in the sticky mesh, and sticky group status.

This section contains the following topics:

- [Displaying DNS Rule Sticky Statistics](#)
- [Displaying Sticky Statistics](#)
- [Displaying Global Sticky Statistics](#)
- [Displaying Global Sticky Mesh Statistics](#)
- [Displaying Sticky Group Statistics](#)
- [Displaying the Sticky Status](#)
- [Displaying the Sticky Database Status](#)
- [Displaying the Global Sticky Operating Status](#)

- [Displaying Global Sticky Mesh Operating Status](#)
- [Displaying Sticky Group Configuration](#)

Displaying DNS Rule Sticky Statistics

You display all DNS sticky lookups by DNS rule name by using the **show statistics dns sticky rule** command.

The syntax for the command is as follows:

```
show statistics dns sticky rule
```

[Table 13-39](#) describes the fields in the **show statistics dns sticky rule** command output.

Table 13-39 *Field Descriptions for show statistics dns sticky rule Command*

Field	Description
Rule	Name of the matched DNS rule.
Hits	Total number of successful lookups in the sticky database for the sticky database entry.
Misses	Total number of failed lookups in the sticky database for the DNS rule.
Additions	Total number of times that a request matched on a DNS rule, resulting in the GSS adding an entry to the sticky database.

Displaying Sticky Statistics

You display general statistics about the sticky database by using the **show statistics sticky** command. This includes statistics such as the total number of hits and misses in the sticky database, number of entries in the sticky database, and total number of lookups.

The syntax for the command is as follows:

```
show statistics sticky
```

Table 13-40 describes the fields in the **show statistics sticky** command output.

Table 13-40 Field Descriptions for show statistics sticky Command

Field	Description
Current entry count	Current number of entries in the sticky database.
Highest entry count	Maximum number of entries in the sticky database since the last time sticky was enabled or the sticky statistics were cleared.
Total Lookups	Total number of lookups in the sticky database.
Hits	Number of successful lookups in the sticky database.
Misses	Number of failed lookups in the sticky database.
Addition success	Number of addition requests for the sticky database that succeeded.
Addition fail	Number of addition requests for the sticky database that failed. The sticky database will not accept further addition requests when the database is full, you stop DNS sticky through the sticky stop CLI command, or there has been an internal error.
Modification success	Number of answer modification requests that succeeded.
Modification fail	Number of answer modification requests that failed.
Timeouts	Number of entries removed from the sticky database because the answer exceeded the user-configured Entry Inactivity Timeout value.
Reclaimed	Number of entries removed from the sticky database due to an overflow.
CLI deletions local	Number of entries manually deleted from the sticky database through the sticky database delete CLI command, entered on the local GSS node.
CLI deletions remote	Number of entries manually deleted from the sticky database through the sticky database delete CLI command, entered on a GSS peer.

Displaying Global Sticky Statistics

You display a summary of counter statistics for global sticky messaging between the local GSS node and its GSS peers by using the **show statistics sticky global** command.

The syntax for the command is as follows:

show statistics sticky global

The **show statistics sticky global** command output is divided into two sets of global sticky message statistics:

- Individual sticky database entry operations performed by the local GSS node
- Sticky database messages sent or received by the local GSS node to or from its GSS peers.

Table 13-41 describes the fields in the **show statistics sticky global** command output.

Table 13-41 Field Descriptions for show statistics sticky global Command

Field	Description
Entry Type	Statistics on sticky database entry operations performed by the local GSS node.
Send OK	Sticky database entry messages transmitted by the local GSS node without a failure.
Send Fail	Sticky database entry messages transmitted by the local GSS node with errors.
Received	Sticky database entry messages received by the local GSS node from GSS peers.
Add	Number of new entries added to the sticky database of the local GSS node.
Modify	Number of sticky database entries modified by the local GSS node due to a keepalive failure.

Table 13-41 Field Descriptions for *show statistics sticky global* Command (continued)

Field	Description
Lookup Fast	Number of sticky database entries in the local GSS node that had their sticky inactivity time reset to an initial value because the GSS performed a fast lookup. A GSS performs a fast lookup when adding new entries to the sticky database, deleting entries from the sticky database, or when the sticky expiration time is less than 5 minutes.
Lookup Slow	Number of sticky database entries in the local GSS node that had their sticky inactivity time reset to an initial value because the GSS performed a slow lookup. A GSS performs a slow lookup when the sticky expiration time is greater than 5 minutes.
Remove	Number of entries removed from the sticky database of the local GSS node through the sticky database delete command. Entries removed by the sticky database delete all command are reflected in the Remove All field (see below).
Add Sync	Number of entries added to the sticky database of the local GSS node due to the result of a peer synchronization, not a normal DNS client request.
Message Type	Statistics on sticky database messages sent or received by the local GSS node.
Send OK	Messages transmitted by the local GSS node without a failure.
Send Fail	Messages transmitted by the local GSS node with errors.
Received	Messages received by the local GSS node from GSS peers.
Add	Number of Add entry type messages sent or received by the local GSS node.
Modify	Number of Modify entry type messages sent or received by the local GSS node.

Table 13-41 Field Descriptions for *show statistics sticky global* Command (continued)

Field	Description
Lookup Fast	Number of Lookup Fast entry type messages sent or received by the local GSS node.
Lookup Slow	Number of Lookup Slow entry type messages sent or received by the local GSS node.
Remove	Number of Remove messages sent or received by the the local GSS node.
Add Sync	Number of Add Sync entry type messages sent or received by the local GSS node.
Remove All	Number of times the sticky database delete all command has been entered on the local GSS node to delete all entries from the sticky database. The Remove All count includes the number of Remove All messages sent and received by the local GSS node.
Request Db	Number of times the local GSS node sent a Request Db message to a GSS peer or received a Request Db message from a GSS peer, requesting to share the contents of its sticky database upon startup.
Ack RequestDb	Number of times the local GSS node sent an Ack RequestDb message to a GSS peer or received an Ack RequestDb message from a GSS peer to acknowledge that it received a request to share the contents of its sticky database upon startup.
Refuse Db Req	Number of times the local GSS node sent a Refuse Db Req message to a GSS peer or received a Refuse Db Req message from a GSS peer, indicating a refusal to share the contents of its sticky database upon startup. A GSS, typically, refuses to share the contents of its local database while in the process of performing a database synchronization.

Table 13-41 Field Descriptions for *show statistics sticky global* Command (continued)

Field	Description
Sync Start	Number of times the Sync Start message has been sent or received by the local GSS node. The GSS uses the Sync Start message to lock out certain critical functions (such as the use of the sticky database delete command) while any GSS within the mesh is performing a synchronization. When the Sync Start message arrives, the GSS blocks all sticky database entry deletions until it either receives the Sync Done message or an internal timer expires.
Sync Done	Number of times the Sync Done message has been sent or received by the local GSS node. The GSS uses the Sync Done message to lock out certain critical functions (such as the use of the sticky database delete command) while any GSS within the mesh is performing a synchronization.
Version mis-match	Error message indicating the number of times the local GSS node was unable to communicate with a peer due to different versions of GSS software.

Table 13-41 Field Descriptions for *show statistics sticky global* Command (continued)

Field	Description
Clock Out Of Sync	Error message indicating the number of times the local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by more than three minutes with the other GSS peers ignores update messages from all peers until you resynchronize its system clock (see Chapter 8, Configuring DNS Sticky , for details).
Mask mis-match	<p>Error message indicating the number of times that the local GSS node was unable to communicate with a peer due to a difference in global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure.</p> <p>You globally configure the subnet mask of all GSS devices in the mesh from the primary GSSM GUI Global Sticky Configuration details page (see Chapter 8, Configuring DNS Sticky, for details).</p>

Displaying Global Sticky Mesh Statistics

You display detailed statistics for each GSS peer in the global sticky mesh by using the **show statistics sticky mesh** CLI command.

Table 13-42 describes the fields in the **show statistics sticky mesh** command output.

Table 13-42 Field Descriptions for show statistics sticky mesh Command

Field	Description
Mesh Information for application sticky	Status and statistics about the global sticky mesh.
Transmit Pkts	Total number of application data packets transmitted by the local GSS node to GSS peers in the mesh.
Transmit Bytes	Total number of application data bytes transmitted by the local GSS node to GSS peers in the mesh.
Receive Pkts	Total number of application data packets received by the local GSS node from GSS peers in the mesh.
Receive Bytes	Total number of application data bytes received by the local GSS node from GSS peers in the mesh.
Dropped Tx Pkts	Total number of packets to be transmitted by the local GSS node but were dropped due to buffer errors.
Dropped Rx Pkts	Total number of packets received by the local GSS node but were dropped due to buffer errors.
Current TxQueue	Total number of packets in the buffer transmit queue of the local GSS node that are waiting to be transmitted.
Maximum TxQueue	Maximum number of packets that have been in the buffer transmit queue of the local GSS node.
Current RxQueue	Total number of packets in the buffer receive queue of the local GSS node that are waiting to be received.
Maximum RxQueue	Maximum number of packets that have been in the buffer receive queue of the local GSS node.

Table 13-42 Field Descriptions for *show statistics sticky mesh* Command (continued)

Field	Description
Buffers Alloc'd	Number of optimal-sized frames allocated for the buffer transmit and buffer receive data.
Buffers Free	Number of buffers currently free in the local GSS node.
Session Information for <i>GSS peer</i>	Status and statistics for a specific GSS peer in the mesh.
GSS ID	Unique identifier of the GSS peer in the mesh.
CurTx Data Pkts	Number of data packets sent by the local GSS node to the GSS peer during the current session.
CurTx Data Bytes	Number of data bytes sent by the local GSS node to the GSS peer during the current session.
TtlTx Data Pkts	Number of application data packets sent by the local GSS node to the GSS peer for the total duration of the mesh.
TtlTx Data Bytes	Number of application data bytes sent by the local GSS node to the GSS peer for the total duration of the mesh.
Transmit Pkts	Total number of packets transmitted from the local GSS node to the GSS peer (including application packets, control packets, RTT packets, and keepalive packets).
Transmit Bytes	Total number of bytes transmitted from the local GSS node to the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes).
CurRx Data Pkts	Number of data packets received by the local GSS node from the GSS peer during the current session.
CurRx Data Bytes	Number of data bytes received by the local GSS node from the GSS peer during the current session.
TtlRx Data Pkts	Number of application data packets received by the local GSS node from the GSS peer for the total duration of the mesh.

Table 13-42 Field Descriptions for *show statistics sticky mesh* Command (continued)

Field	Description
TtlRx Data Bytes	Number of application data bytes received by the local GSS node from the GSS peer for the total duration of the mesh.
Receive Pkts	Total number of packets received by the local GSS node from the GSS peer (including application packets, control packets, RTT packets, and keepalive packets).
Receive Bytes	Total number of bytes received by the local GSS node from the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes).
ConnectFailures	Number of times that the connection attempt failed between the local GSS node and the GSS peer.
CurConnAttempts	Number of current connection attempts between the local GSS node and the GSS peer.
ConnectRejects	Number of connections rejected by the GSS peer.
ConnectDeclines	Number of connections declined by the local GSS node.

Displaying Sticky Group Statistics

You display a summary of statistics for all configured sticky groups by using the **show statistics sticky group-summary** command.

[Table 13-43](#) describes the fields in the **show statistics sticky group-summary** command output.

Table 13-43 Field Descriptions for *show statistics sticky group-summary* Command

Field	Description
Group Name	Unique alphanumeric name of the DNS sticky group.
Group Number	IP address block of the sticky group, specified in dotted-decimal notation.

Table 13-43 Field Descriptions for show statistics sticky group-summary Command (continued)

Field	Description
Total Entries	The total number of D-proxy IP address and subnet mask pairs contained in the sticky group.
Total Hits	Accumulated hit count for all entries in the sticky group. Increments when a match occurs for each sticky group entry

You display statistics for a specific sticky group by using the **show statistics sticky group-name** command.

The syntax for the command is as follows:

```
show statistics sticky group-name {groupname}
```

The *groupname* argument specifies the exact name of a sticky group in order to display all sticky entries related to that group.

[Table 13-44](#) describes the fields in the **show statistics sticky group-name** command output.

Table 13-44 Field Descriptions for show statistics sticky group-name Command

Field	Description
Group Name	Unique alphanumeric name of the DNS sticky group.
Group Number	IP address block of the sticky group, specified in dotted-decimal notation
Total Entries for Group	Total number of D-proxy IP addresses included in the sticky group.
Address	D-proxy IP address included in the sticky group.
Prefix	Subnet mask included in the sticky group, displayed as an integer (for example, 24 or 32).
Hit Count	Number that increments when a match occurs for this sticky group entry.
Last Time Hit	Last time that the hit count incremented due to an entry match.

Displaying the Sticky Status

You display general status information about the sticky subsystem by using the **show sticky** command.

The syntax for the command is as follows:

```
show sticky
```

[Table 13-45](#) describes the fields in the **show sticky** command output.

Table 13-45 Field Descriptions for show sticky Command

Field	Description
Sticky Manager status	<p>Current operating status of the Sticky Manager component. The Sticky Manager is responsible for maintaining and managing the sticky database in the GSS. Status messages are as follows:</p> <ul style="list-style-type: none"> • Initializing—Appears only during boot time or after entering the gss start CLI command. • Disabled via GUI—Appears after you disable sticky from the primary GSSM GUI. • Stopped via CLI—Appears after you enter the sticky stop CLI command. • Ready in Local mode—Appears when the GSS is configured for sticky Local mode from the primary GSSM GUI and the GSS software is running. • Ready in Global mode—Appears when the GSS is configured for sticky Global mode from the primary GSSM GUI and the GSS software is running.
Database entry count	Current number of entries in the sticky database.

Table 13-45 Field Descriptions for show sticky Command (continued)

Field	Description
Dump status	Current sticky database dump subsystem status of the GSS. The GSS automatically dumps sticky database entries to a backup file on disk approximately every 20 minutes. The Dump status messages include Initialized, Disabled, Waiting, and In Progress.
Dump interval	Time period between automatic sticky database dumps performed by the GSS.
Reclaim status	Current operating status of the overflow recovery subsystem. The Reclaim status messages include Initialized, Disabled, Waiting, and In Progress.
Timeout status	Current operating status of the entry inactivity timeout subsystem. The Timeout status messages include Initialized, Disabled, Waiting, and In Progress.
Timeout interval	Time period between checks by the GSS to verify when the user-configured sticky inactivity timeout value elapses.
Mesh status	Current operating status of the sticky global mesh. Status messages are as follows: <ul style="list-style-type: none"> • Running—The GSS is operating properly in the sticky mesh. • Failed—The GSS is unable to operate properly in the sticky mesh. • Waiting—The GSS is waiting for mesh configuration information. • Enabled—Global sticky is enabled on the local GSS node. • Disabled—Global sticky is disabled on the local GSS node (either from the primary GSSM GUI or through the sticky stop CLI command).

Displaying the Sticky Database Status

You display sticky database entries by specifying one or more entry matching criteria by using the **show sticky database** command.

The syntax for the command is as follows:

```
show sticky database {all | answer {name/ip_address} | domain {name} |  
  domain-list {name} | group {name} | inactive minimum {minutes} |  
  maximum {minutes} | ip {ip_address} netmask {netmask} | rule  
  {rule_name}}
```

The keywords and arguments are:

- **all**—Displays all sticky entries in the sticky database.
- **answer** *name/ip_address*—Displays all sticky entries related to a particular answer. Specify the name of the answer. If there is no name for the answer, specify the IP address of the sticky answer in dotted-decimal notation (for example, 192.168.9.0).
- **domain** *name*—Displays all sticky entries related to a domain. Specify the exact name of a previously created domain.
- **domain-list** *name*—Displays all sticky entries related to a domain list. Specify the exact name of a previously created domain list.
- **group** *name*—Displays all sticky entries related to a sticky group. Specify the exact name of a previously created sticky group.
- **inactive minimum** *minutes* **maximum** *minutes*—Displays all sticky entries that have not received a client hit in the time interval between the specified minimum and maximum values, entered in minutes. Enter a value from 0 to 10100 minutes (7 days) as the specified minimum value and maximum value.
- **ip** *ip_address* **netmask** *netmask*—Displays all sticky entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **rule** *rulename*—Displays all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

Table 13-46 describes the fields in the **show sticky database all** command output.

Table 13-46 Field Descriptions for show sticky database all Command

Field	Description
Client/Group	IP address of client D-proxy or name of sticky group.
Domain/DL	Name of the hosted domain (including wildcards) or the name of a matched domain list (DL).
Rule	Name of the DNS rule that was matched to add this entry.
Answer	VIP address of the answer (VIP-type answer).
SIT	User-specified sticky interval timeout (SIT) value.
TTL	Remaining time that the entry in the sticky database is valid.
Hits	Total number of successful lookups in the sticky database for the sticky database entry.

Displaying the Global Sticky Operating Status

You display the most recent sticky database message identifiers sent by the local GSS node and received from its GSS mesh peers by using the **show sticky global** command. Message identifiers can be helpful when you need to verify the most recent sticky database messages sent from and received by the local GSS node.

You display a more detailed listing of recent global sticky message identifiers by specifying the **verbose** keyword.

The syntax for the command is as follows:

```
show sticky global [verbose]
```

Table 13-47 describes the fields in the **show sticky global** command output.

Table 13-47 Field Descriptions for show sticky global Command

Field	Description
Mesh Peer Count	Total number of GSS peers in a sticky mesh (not including the local GSS node).
Last Message ID Sent for Each Message Type	Summary of the unique global sticky message identifiers last sent by the local GSS node.
Add	Unique identifier of the last Add entry-type message sent by the local GSS node.
Modify	Unique identifier of the last Modify entry-type message sent by the local GSS node.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.
Details of Most Recently Received Messages by Peer	Status summary of the global sticky message identifiers last received by the local GSS node.
Peer Name	Hostname of the GSS peer in the mesh.
Peer ID	Unique identifier of the GSS peer in the mesh.
Last Type	Type of the message last received from the peer.

Table 13-47 Field Descriptions for show sticky global Command (continued)

Field	Description
Last Status	<p>Status of the last message received from the peer. Status messages are as follows:</p> <ul style="list-style-type: none"> • Received OK—Message was received and processed • Version mismatch—Message dropped because the local GSS node was unable to communicate with a peer due to different versions of the GSS software. • Clock out of sync—The local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by more than 3 minutes with the other GSS peers ignores update messages from all peers until you resynchronize its system clock (see Chapter 8, Configuring DNS Sticky, for details). • Mask mismatch—Local GSS node was unable to communicate with a peer due to a difference in global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure. See Chapter 8, Configuring DNS Sticky, for details about globally configuring the subnet mask of all GSS devices in the mesh from the primary GSSM GUI.
Last MessageID Received for each Message Type...	Summary of the unique global sticky messages last received by the local GSS node from each GSS mesh peer.
Add	Unique identifier of the last Add entry-type message received by the local GSS node from the GSS peer.

Table 13-47 Field Descriptions for show sticky global Command (continued)

Field	Description
Modify	Unique identifier of the last Modify entry-type message received by the local GSS node from the GSS peer.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message received by the local GSS node from the GSS peer.

Table 13-48 describes the fields in the **show sticky global verbose** command output.

Table 13-48 Field Descriptions for show sticky global verbose Command

Field	Description
Mesh Peer Count	Total number of GSS peers in a sticky mesh (not including the local GSS node).
Last Message ID Sent for Each Message Type	Summary of the unique global sticky message identifiers last sent by the local GSS node.
Add	Unique identifier of the last Add entry-type message sent by the local GSS node.
Modify	Unique identifier of the last Modify entry-type message sent by the local GSS node.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.
Lookup Slow	Unique identifier of the last Lookup Slow entry-type message sent by the local GSS node.
Remove	Unique identifier of the last Remove entry-type message sent by the local GSS node.
Add Sync	Unique identifier of the last Add Sync entry-type message sent by the local GSS node.
Remove All	Unique identifier of the last Remove All message sent by the local GSS node.

Table 13-48 Field Descriptions for *show sticky global verbose* Command (continued)

Field	Description
Request Db	Unique identifier of the last Request Db message sent by the local GSS node.
Ack ReqDb	Unique identifier of the last Ack ReqDb message sent by the local GSS node.
Refuse ReqDb	Unique identifier of the last Refuse ReqDb message sent by the local GSS node.
Sync Start	Unique identifier of the last Sync Start message sent by the local GSS node.
Sync Done	Unique identifier of the last Sync Done message sent by the local GSS node.
Details of Most Recently Received Messages by Peer	Status summary of the global sticky message identifiers last received by the local GSS node.
Peer Name	Hostname of the GSS peer in the mesh.
Peer ID	Unique identifier of the GSS peer in the mesh.
Last Type	Type of the message last received from the peer.

Table 13-48 Field Descriptions for *show sticky global verbose* Command (continued)

Field	Description
Last Status	<p>Status of the last message received from the peer. Status messages are as follows:</p> <ul style="list-style-type: none"> • Received OK—Message was received and processed • Version mismatch—Message dropped because the local GSS node was unable to communicate with a peer due to different versions of the GSS software. • Clock out of sync—The local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by more than 3 minutes with the other GSS peers ignores update messages from all peers until you resynchronize its system clock (see Chapter 8, Configuring DNS Sticky, for details). • Mask mismatch—The local GSS node was unable to communicate with a peer due to a difference in global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure. See Chapter 8, Configuring DNS Sticky, for details about globally configuring the subnet mask of all GSS devices in the mesh from the primary GSSM GUI .
Last MessageID Received for each Message Type...	Summary of the unique global sticky messages last received by the local GSS node from each GSS mesh peer.

Table 13-48 Field Descriptions for show sticky global verbose Command (continued)

Field	Description
Add	Unique identifier of the last Add entry-type message received by the local GSS node from the GSS peer.
Modify	Unique identifier of the last Modify entry-type message received by the local GSS node from the GSS peer.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message received by the local GSS node from the GSS peer.
Lookup Slow	Unique identifier of the last Lookup Slow entry-type message received by the local GSS node from the GSS peer.
Remove	Unique identifier of the last Remove entry-type message received by the local GSS node from the GSS peer.
Add Sync	Unique identifier of the last Add Sync entry-type message received by the local GSS node from the GSS peer.
Remove All	Unique identifier of the last Remove All message received by the local GSS node from the GSS peer.
Request Db	Unique identifier of the last Request Db message received by the local GSS node from the GSS peer.
Ack ReqDb	Unique identifier of the last Ack RegDb message received by the local GSS node from the GSS peer.
Refuse Db	Unique identifier of the last Refuse ReqDb message received by the local GSS node from the GSS peer.
Sync Start	Unique identifier of the last Sync Start message received by the local GSS node from the GSS peer.
Sync Done	Unique identifier of the last Sync Done message received by the local GSS node from the GSS peer.

Displaying Global Sticky Mesh Operating Status

You display sticky mesh status information locally from the CLI of a GSS by using the **show sticky mesh** CLI command. This command displays the operating status of the individual GSS peers in the sticky mesh and their connection status to the local GSS node.

The syntax for this command is as follows:

- **show sticky mesh**—Displays a summary of the GSS devices in the sticky mesh and their operating status.
- **show sticky mesh session *session_ID***—Displays operating status information for a specific session ID, which is the point-to-point connection between the local GSS node and a sticky mesh peer. To locate the session ID for a specific GSS peer in the mesh, use the **show sticky mesh** command.
- **show sticky mesh session *session_ID* verbose**—Displays more detailed operating status information for a specific session ID. To locate the session ID for a specific GSS peer in the mesh, use the **show sticky mesh** command.
- **show sticky mesh verbose**—Displays detailed operating status information for the sticky mesh and for all GSS peers in the mesh.

Table 13-49 describes the fields in the **show sticky mesh** command output.

Table 13-49 Field Descriptions for show sticky mesh Command

Field	Description
My GSS ID	Unique identifier of the local GSS node in the mesh.
Mesh ID	Unique identifier of the global sticky mesh.
Port	TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user-configurable.
Remote GSS IP Address/Host Name	IP address or hostname of the GSS peer in the mesh.

Table 13-49 Field Descriptions for show sticky mesh Command (continued)

Field	Description
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.
State	<p data-bbox="653 367 1240 456">State of the communication link between the local GSS node and the mesh peer. The possible states include:</p> <ul data-bbox="666 477 1231 886" style="list-style-type: none"> <li data-bbox="666 477 1231 532">• SESSION_STOP—Indicates that the session is dead <li data-bbox="666 553 1231 609">• SESSION_INIT—Indicates that the session is initializing <li data-bbox="666 630 1231 685">• SESSION_OPEN—Indicates that the connection to the peer has been made <li data-bbox="666 706 1231 761">• SESSION_AUTH—Indicates that authentication is occurring <li data-bbox="666 782 1231 813">• SESSION_UP—Indicates that the session is up <li data-bbox="666 834 1231 889">• SESSION_DOWN—Indicates that the session is down or failing

Table 13-50 describes the fields in the **show sticky mesh session** command output.

Table 13-50 Field Descriptions for show sticky mesh session Command

Field	Description
Session Information for <i>GSS peer</i>	Hostname of the GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.
RTT	Application-level round-trip time (RTT) between the local GSS node and the mesh peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.
State	State of the communication link between the local GSS node and the mesh peer. Possible states are as follows: <ul style="list-style-type: none"> • SESSION_STOP—Indicates that the session is dead • SESSION_INIT—Indicates that the session is initializing • SESSION_OPEN—Indicates that the connection to the peer has been made • SESSION_AUTH—Indicates that authentication is occurring • SESSION_UP—Indicates that the session is up • SESSION_DOWN—Indicates that the session is down or failing
IP Address	IP address of the GSS peer.
GSS ID	Unique identifier of the GSS peer in the mesh.

Table 13-51 describes the fields in the **show sticky mesh session verbose** command output.

Table 13-51 Field Descriptions for show sticky mesh session verbose Command

Field	Description
Session Information for <i>GSS peer</i>	Hostname of the GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.
Session State	State of the communication link between the local GSS node and the mesh peer. Possible states are as follows: <ul style="list-style-type: none"> • SESSION_STOP—Indicates that the session is dead • SESSION_INIT—Indicates that the session is initializing • SESSION_OPEN—Indicates that the connection to the peer has been made • SESSION_AUTH—Indicates that authentication is occurring • SESSION_UP—Indicates that the session is up • SESSION_DOWN—Indicates that the session is down or failing
RTT	Application-level round-trip time (RTT) between the local GSS node and the mesh peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.
Encrypt Type	Encryption method performed on the data packets. The method is one of the following: <ul style="list-style-type: none"> • md5hash—MD5-based hashing encryption method • none—No encryption See Chapter 8, Configuring DNS Sticky for details.

Table 13-51 Field Descriptions for show sticky mesh session verbose Command (continued)

Field	Description
Authentication	Authentication method performed by the GSS peer to prevent unauthorized access. The method is one of the following: <ul style="list-style-type: none"> challenge—Challenge Handshake Authentication Protocol (CHAP) none—No secret string used for authentication See Chapter 8, Configuring DNS Sticky for details.
KalFreq	Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user configurable.
Max FrameSize	Maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user-configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.
PrePend	Allocated header size in the buffer. The header size is always 8 bytes.
IP Address	IP address of the GSS peer in the mesh.
GSS ID	Unique identifier of the GSS peer in the mesh.
Connect from IP	Actual IP network address of the GSS peer in the mesh.
My Local Address Via Peer	IP address of the local GSS node as seen by the GSS peer.
Last Up Event	Day and time of the most recent Up event.
Last Down Event	Day and time of the most recent Down event.
FSM Events	Finite State Machine events as related to the Session State field.
STOP	Number of SESSION_STOP events.
INIT	Number of SESSION_INIT events.

Table 13-51 Field Descriptions for show sticky mesh session verbose Command (continued)

Field	Description
OPEN	Number of SESSION_OPEN events.
AUTH	Number of SESSION_AUTH events.
UP	Number of SESSION_UP events.
DOWN	Number of SESSION_DOWN events.

[Table 13-52](#) describes the fields in the **show sticky mesh verbose** command output.

Table 13-52 Field Descriptions for show sticky mesh verbose Command

Field	Description
Mesh Information for application sticky	Status and statistics about the global sticky mesh.
My GSS ID	Unique identifier of the local GSS node in the mesh.
Mesh ID	Unique identifier of the global sticky mesh.
Port	TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user configurable.
Encrypt Type	Encryption method performed on the data packets. The method is one of the following: <ul style="list-style-type: none"> md5hash—MD5-based hashing encryption method none—No encryption See Chapter 8, Configuring DNS Sticky for details.

Table 13-52 Field Descriptions for *show sticky mesh verbose* Command (continued)

Field	Description
Authentication	<p>Authentication method performed by GSS peers to prevent unauthorized access. The method is one of the following:</p> <ul style="list-style-type: none"> challenge—Challenge Handshake Authentication Protocol (CHAP) none—No secret string used for authentication <p>See Chapter 8, Configuring DNS Sticky for details.</p>
KalFreq	Time in seconds between sending keepalive messages to GSS peers. This parameter is not user configurable and always displays as “default”.
MaxFrameSize	Maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.
Max Rate	Maximum rate that the local GSS node can transmit packets to GSS peers in the mesh.
Favored Peer	Favored GSS peer for the local GSS node, specified on the Global Sticky Configuration details page of the primary GSSM GUI. A favored peer enables you to force a faster synchronization of sticky database entries with a specific GSS peer upon reentry into the sticky mesh. If you did not specify a favored peer, the GSS displays “No Favored Peer configured.”
Session Information for GSS peer	Status and statistics for a specific GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.

Table 13-52 Field Descriptions for *show sticky mesh verbose* Command (continued)

Field	Description
Session State	<p>State of the communication link between the local GSS node and the mesh peer. Possible states are as follows:</p> <ul style="list-style-type: none"> • SESSION_STOP—Indicates that the session is dead • SESSION_INIT—Indicates that the session is initializing • SESSION_OPEN—Indicates that the connection to the peer has been made • SESSION_AUTH—Indicates that authentication is occurring • SESSION_UP—Indicates that the session is up • SESSION_DOWN—Indicates that the session is down or failing
RTT	<p>Application-level round-trip time (RTT) between the local GSS node and this GSS peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.</p>
Encrypt Type	<p>Encryption method performed on the data packets. The method is one of the following:</p> <ul style="list-style-type: none"> • md5hash—MD5-based hashing encryption method • none—No encryption <p>See Chapter 8, Configuring DNS Sticky for details.</p>

Table 13-52 Field Descriptions for *show sticky mesh verbose* Command (continued)

Field	Description
Authentication	Authentication method performed by GSS peers to prevent unauthorized access. The method is one of the following: <ul style="list-style-type: none"> challenge—Challenge Handshake Authentication Protocol (CHAP) none—No secret string used for authentication See Chapter 8, Configuring DNS Sticky for details.
KalFreq	Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user configurable.
Max FrameSize	Maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.
PrePend	Allocated header size in the buffer. The header size is always 8 bytes.
IP Address	IP address of the GSS peer in the mesh.
GSS ID	Unique identifier of the GSS peer in the mesh.
Connect from IP	Actual IP network address of the GSS peer in the mesh.
My Local Address Via Peer	IP address of the local GSS node as seen by the GSS peer.
Last Up Event	Day and time of the most recent Up event.
Last Down Event	Day and time of the most recent Down event.
FSM Events	Finite State Machine events as related to the Session State field.
STOP	Number of SESSION_STOP events.
INIT	Number of SESSION_INIT events.

Table 13-52 Field Descriptions for *show sticky mesh verbose* Command (continued)

Field	Description
OPEN	Number of SESSION_OPEN events.
AUTH	Number of SESSION_AUTH events.
UP	Number of SESSION_UP events.
DOWN	Number of SESSION_DOWN events.

Displaying Sticky Group Configuration

You display a summary of all configured sticky groups by using the **show sticky group-summary** command.

[Table 13-53](#) describes the fields in the **show sticky group-summary** command output.

Table 13-53 Field Descriptions for *show sticky group-summary* Command

Field	Description
Name	Unique alphanumeric name of the DNS sticky group.
Address Blocks	IP address block of the sticky group, specified in dotted-decimal notation.

You display the configuration of a specific sticky group by using the **show sticky group-name** command.

The syntax for the command is as follows:

```
show sticky group-name {groupname}
```

The *groupname* argument specifies the exact name of a sticky group in order to display all sticky entries related to that group.

[Table 13-54](#) describes the fields in the **show sticky group-name** command output.

Table 13-54 Field Descriptions for show sticky group-name Command

Field	Description
Name	Unique alphanumeric name of the DNS sticky group.
Address Blocks	IP address block of the sticky group, specified in dotted-decimal notation.

Clearing GSS Global Server Load-Balancing Statistics

You reset global server load-balancing statistics for one or more of your GSS components by using the **clear statistics** command. Clearing the statistics for a GSS component erases all record of routing activity and performance for that device.

The syntax for the **clear statistics** command is as follows:

```
clear statistics {boomerang | ddos [all | attacks | drops | global ] | dns |
  drpagent | keepalive {all | cra | http-head | icmp | kalap | ns |
  scripted-kal | tcp} | proximity | sticky {mesh}}
```

The keywords are as follows:

- **boomerang**—Resets statistics that relate to the Boomerang server component of the GSS.
- **ddos**—Resets statistics that relate to the DDoS detection and mitigation component of the GSS.
- **global**—Resets global statistics for the GSS DDoS detection and mitigation component.
- **attacks**—Resets attack statistics for the GSS DDoS detection and mitigation component.
- **dns**—Resets statistics that relate to the DNS server component of the GSS, including proximity and sticky DNS rule statistics.
- **drpagent**—Resets statistics that relate to the DRP agent component of the GSS.
- **keepalive**—Resets statistics that relate to the keepalive function of the GSS software.

- **all**—Resets statistics for all keepalive types maintained by the GSS.
- **cra**—Resets statistics for only CRA-type keepalives maintained by the GSS.
- **http-head**—Resets statistics for only the VIP HTTP-HEAD type keepalive maintained by the GSS.
- **icmp**—Resets statistics for only the VIP ICMP-type keepalive maintained by the GSS.
- **kalap**—Resets statistics for only the VIP KAL-AP-type keepalive maintained by the GSS.
- **ns**—Resets statistics for the Name Server-type keepalive maintained by the GSS.
- **scripted-kal**—Resets statistics for the Scripted-Kal -type keepalive maintained by the GSS.
- **tcp**—Resets statistics for the IP and port TCP-type keepalive maintained by the GSS
- **proximity**—Resets statistics for the network proximity function.
- **sticky**—Resets statistics for the DNS sticky function.
- **mesh**—Resets sticky global mesh and session statistics for the local GSS node of the mesh.

For example, enter:

```
gss1.yourdomain.com# clear statistics keepalive tcp  
Are you sure? (yes/no) yes  
tcp keepalive statistics cleared
```

or

```
gss1.yourdomain.com# clear statistics proximity  
Are you sure? (yes/no) yes  
proximity statistics cleared
```

Displaying Global Server Load-Balancing Statistics from the GUI

From the Monitoring tab of the primary GSSM GUI, you can display the status of global load balancing on your GSS network using a variety of functions that filter and condense GSS traffic and statistics. These statistics provide you with an overview of the online status of your resources (such as answers, keepalives, DNS rules, hosted domains, and source addresses). You can also display advanced traffic management functions, such as DNS sticky and network proximity, for the GSS network.

This section contains the following topics:

- [Displaying Answer Status and Statistics](#)
- [Displaying DNS Rule Statistics](#)
- [Displaying Domain Hit Counts](#)
- [Displaying Global Statistics](#)
- [Displaying Source Address Statistics](#)
- [Displaying DDoS Statistics](#)

Displaying Answer Status and Statistics

The Answers section of the Monitoring tab displays statistics about the answer resources in your GSS network. Answer resources also include statistics about keepalive probes directed to the answer resource.

This section contains the following topics:

- [Displaying Answer Hit Counts](#)
- [Displaying Answer Keepalive Statistics](#)
- [Displaying the Answer Status](#)

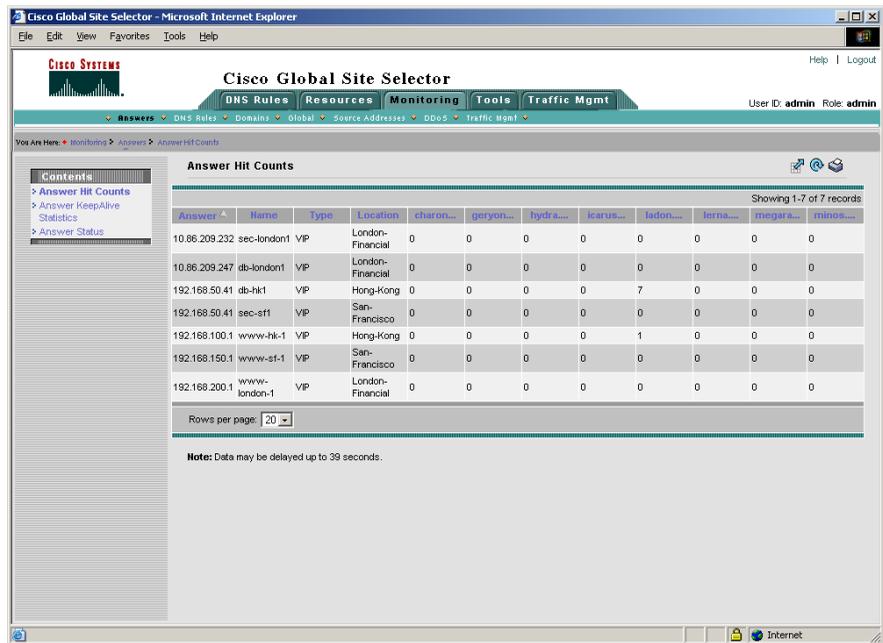
Displaying Answer Hit Counts

The Answer Hit Counts list page displays statistics about the GSS answer resources and the number of times that user requests have been directed to each answer resource. Answer hit counts allow you to gauge how well your GSS resources respond to user requests.

To display the number of hits recorded by each answer, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Answers** navigation link.
3. Click the **Answer Hit Counts** navigation link (located in the Contents list). The Answer Hit Counts list page appears (see [Figure 13-1](#)).

Figure 13-1 Answer Hit Counts List Page



The screenshot shows the Cisco Global Site Selector GUI in Microsoft Internet Explorer. The main navigation tabs are DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. The Monitoring tab is active, and the Answers navigation link is selected. The Answer Hit Counts page is displayed, showing a table with the following data:

Answer	Name	Type	Location	charon...	geron...	hydra...	leatus...	ladon...	lerna...	megara...	minos...
10.86.209.232	sec-london1	VIP	London-Financial	0	0	0	0	0	0	0	0
10.86.209.247	db-london1	VIP	London-Financial	0	0	0	0	0	0	0	0
192.168.50.41	db-hk1	VIP	Hong-Kong	0	0	0	0	7	0	0	0
192.168.50.41	sec-sf1	VIP	San-Francisco	0	0	0	0	0	0	0	0
192.168.100.1	www-hk-1	VIP	Hong-Kong	0	0	0	0	1	0	0	0
192.168.150.1	www-sf-1	VIP	San-Francisco	0	0	0	0	0	0	0	0
192.168.200.1	www-london-1	VIP	London-Financial	0	0	0	0	0	0	0	0

The table shows 7 records. The 'Rows per page' is set to 20. A note at the bottom states: 'Note: Data may be delayed up to 39 seconds.'

24/01/22

Table 13-55 describes the fields on the Answer Hit Counts list page.

Table 13-55 Field Descriptions for Answer Hit Counts List Page

Field	Description
Answer	IP address of the answer resource.
Name	Name assigned to the answer using the primary GSSM GUI.
Type	Resources to which the GSS resolves DNS requests. The answer types include: VIP, CRA, or Name Server.
Location	GSS network location of the answer.
Name of the GSS or GSSM	Number of requests directed to the answer by each GSS device.

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

Displaying Answer Keepalive Statistics

The Answer Keepalive Statistics list page displays statistics about keepalive probes sent to the answer resource by each GSS in the network. For each answer configured on your GSS, the Answer Keepalive Statistics list page displays the number of keepalive probes directed to that answer by the primary and the standby GSSM as well as information about how that keepalive probe was handled. The Answer Keepalive Statistics list page also displays multiple keepalives if assigned for a single VIP answer.

You may discover that certain answers may be offline or have problems staying online if a large number of keepalive probes are rejected or encounter transition conditions.

To display the keepalive statistics for each answer, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Answers** navigation link.

- Click the **Answer KeepAlive Statistics** navigation link (located in the Contents list). The Answer KeepAlive Statistics list page appears (see Figure 13-2).

Figure 13-2 Answer Keepalive Statistics List Page

Answer	Type	Name	KeepAlive	Method	Location	charo...	gtpo...	hydra...	icar...	iadon...	ierna...	imegar...	imins...
10.86.209.232	VIP	sec-london1	10.86.209.232	HTTP HEAD to VIP	London-Financial	12,878 0 6,439 1	12,878 0 6,439 1	12,878 0 6,439 1	12,874 0 6,437 1	12,878 0 6,439 1	12,878 0 6,439 1	12,878 0 6,439 1	7,435 0 3,717 1
10.86.209.247	VIP	db-london1	10.86.209.247	TCP to VIP	London-Financial	12,880 0 6,439 1	12,880 0 6,439 1	12,875 0 6,440 1	12,874 0 6,437 1	12,880 0 6,439 1	12,878 0 6,439 1	12,879 0 6,439 1	7,435 0 3,717 1
192.168.1.2	CRA	CRA Answer #2	192.168.1.2	CRA	San-Francisco	42,285 0 42,284 0	42,286 0 42,285 0	42,284 0 42,283 0	42,266 0 42,267 0	42,285 0 42,284 0	42,284 0 42,283 0	42,284 0 42,283 0	29,723 0 29,722 0
192.168.50.41	VIP	db-hk1	192.168.50.41	TCP to VIP	Hong-Kong	51,516 38,637 12,878 0 1	51,516 38,637 12,878 0 1	51,512 38,634 12,874 0 1	51,496 38,622 12,874 0 1	51,516 38,637 12,878 0 1	51,512 38,634 12,877 0 1	51,512 38,634 12,878 0 1	29,740 22,305 7,435 0 1
192.168.50.41	VIP	sec-st1	192.168.50.41	HTTP HEAD to VIP	San-Francisco	64,395 90,153 12,878 0 1	64,395 90,153 12,878 0 1	64,388 90,142 12,878 0 1	64,358 90,094 12,874 0 1	64,395 90,153 12,878 0 1	64,382 90,133 12,877 0 1	64,384 90,137 12,877 0 1	37,173 52,041 7,435 0 1
192.168.100.1	VIP	www-hk-1	192.168.1.45	KAL-AP by VIP	Hong-Kong	177,128 177,127 177,127 1 2	177,129 177,128 177,182 1 2	177,184 177,182 177,057 1 2	177,058 177,128 177,057 1 2	177,129 177,128 177,128 1 2	177,117 177,116 177,116 1 2	177,248 177,247 177,247 1 2	102,255 102,255 102,255 0 0

Table 13-56 describes the fields on the Answer KeepAlive Statistics list page.

Table 13-56 Field Descriptions for Answer Keepalive Statistics List Page

Field	Description
Answer	IP address of the answer resource probed by the GSS.
Type	Resources to which the GSS resolves DNS requests. The answer types include VIP, CRA, or Name Server.
Name	Name assigned to the answer using the primary GSSM GUI.

Table 13-56 Field Descriptions for Answer Keepalive Statistics List Page

Field	Description
Keepalive	Address assigned to the remote device, CRA, or name server that the GSS is to forward requests.
Method	Keepalive method used by the answer: VIP (virtual IP address), NS (name server), or CRA (content routing agent).
Location	GSS network location of the answer.
Name of the GSS or GSSM	<p>Number of keepalive probes directed to the answer by each GSS device and the record of how those probes were handled. Statistics are presented in the following order:</p> <ul style="list-style-type: none"> • Keepalive packets sent—Total number of keepalive probes sent to the answer by each GSS on the network • Keepalive packets received—Total number of keepalive probes returned from the answer • Keepalive positive probe count—Total number of keepalive probes received by the GSS to which a positive (OK) response was returned • Keepalive negative probe count—Total number of keepalive probes received by the GSS to which a negative response was returned • Keepalive transition count—Total number of keepalive probe transitions (for example, from the INIT to the ONLINE state) experienced by the keepalive

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

Displaying the Answer Status

The Answer Status list page displays statistics about the GSS answer resources. Answers can be sorted by IP address, name, type, location, or online status according to a particular device.

To display the status of your GSS answers, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Answers** navigation link.
3. Click the **Answer Status** navigation link (located in the Contents list). The Answer Status list page appears (see [Figure 13-3](#)).

Figure 13-3 Answer Status List Page

The screenshot shows the Cisco Global Site Selector GUI. The breadcrumb trail is "You Are Here: DNS Rules > Answers". The table below shows the answer resources:

IP Address	Name	Status	Type	Location	KeepAlive Method
10.86.209.232	sec-london1	Active	VIP	London-Financial	HTTP HEAD to VIP
10.86.209.247	db-london1	Active	VIP	London-Financial	TCP to VIP
192.168.50.41	db-hk1	Active	VIP	Hong-Kong	TCP to VIP
192.168.50.41	sec-sf1	Active	VIP	San-Francisco	HTTP HEAD to VIP
192.168.100.1	www-hk-1	Active	VIP	Hong-Kong	KAL-AP by VIP
192.168.150.1	www-sf-1	Active	VIP	San-Francisco	KAL-AP by VIP
192.168.200.1	www-london-1	Active	VIP	London-Financial	KAL-AP by VIP

The table indicates it is showing 1-7 of 7 records. The rows per page are set to 20.

240121

Table 13-57 describes the fields on the Answer Status list page.

Table 13-57 Field Descriptions for Answer Status List Page

Field	Description
Answer	IP address of the answer resource.
Name	Name assigned to the answer using the primary GSSM GUI.
Type	Resources to which the GSS resolves DNS requests. The answer types include VIP, CRA, or Name Server.
Location	GSS network location of the answer.
Name of the GSS or GSSM	Online status of the answer according to the named device.

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

Displaying DNS Rule Statistics

The DNS Rule Statistics list page displays statistics about the DNS rules, such as how many queries were processed by each DNS rule and how many of those processed queries were successfully matched with answers.

To display the status of your DNS rules, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **DNS Rules** navigation link. The DNS Rule Statistics list page appears (see Figure 13-4).

Figure 13-4 DNS Rule Statistics List Page



Table 13-58 describes the fields on the DNS Rule Statistics list page.

Table 13-58 Field Descriptions for DNS Rule Statistics List Page

Field	Description
Name	Name assigned to the answer using the primary GSSM.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	Total hit count and successful hit count for the DNS rule from the listed GSS device. Refer to the legend that appears below the listed DNS rules for information about identifying which value represents total hits and which value represents successful DNS requests served.

- Click the column header of any of the displayed columns to sort your DNS rules by a particular property.

Displaying Domain Hit Counts

The Domain Hit Counts list page displays statistics about the hosted domains that the GSS serves and information about how many queries were directed to each domain by each DNS rule. The domain hit counts function tracks the traffic directed to the individual domains, not GSS domain lists, which may include one or more domains.

To display the status of your hosted domains, perform the following steps:

- From the primary GSSM GUI, click the **Monitoring** tab.
- Click the **Domains** navigation link. The Domain Hit Counts list page appears (see [Figure 13-5](#)).

Figure 13-5 Domain Hit Counts List Page

The screenshot shows the Cisco Global Site Selector GUI in Microsoft Internet Explorer. The page title is "Domain Hit Counts". The navigation menu includes "DNS Rules", "Resources", "Monitoring", "Tools", and "Traffic Mgmt". The user is logged in as "admin". The main content area displays a table with the following data:

Domain	echaron.r1	geryon.r1	tydi.s.r1	icarus.r1	hadon.d.s	lerna.s.r1	megara.d.s	mimos.r1
database.myco.com	0	0	0	0	7	0	0	0
www.myco.com	0	0	0	0	1	0	0	0

Rows per page: 20

Note: Data may be delayed up to 39 seconds.

Table 13-59 describes the fields on the Domain Hit Counts list page.

Table 13-59 Field Descriptions for Domain Hit Counts List Page

Field	Description
Domain	DNS domains for which the GSS is responsible. These are the domains contained in your domain lists.
Name of the GSS or GSSM	Total number of requests for the listed domain from each GSS device.

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

Displaying Global Statistics

The Global Statistics list page displays statistics about the GSS network. Global statistics include the average number of DNS requests received by each GSS device and keepalive probes sent to your answers, as well as the online status of each GSS device.

To display the status of your GSS network, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Global** navigation link. The Global Statistics list page (see Figure 13-6) appears.

Figure 13-6 Global Statistics List Page

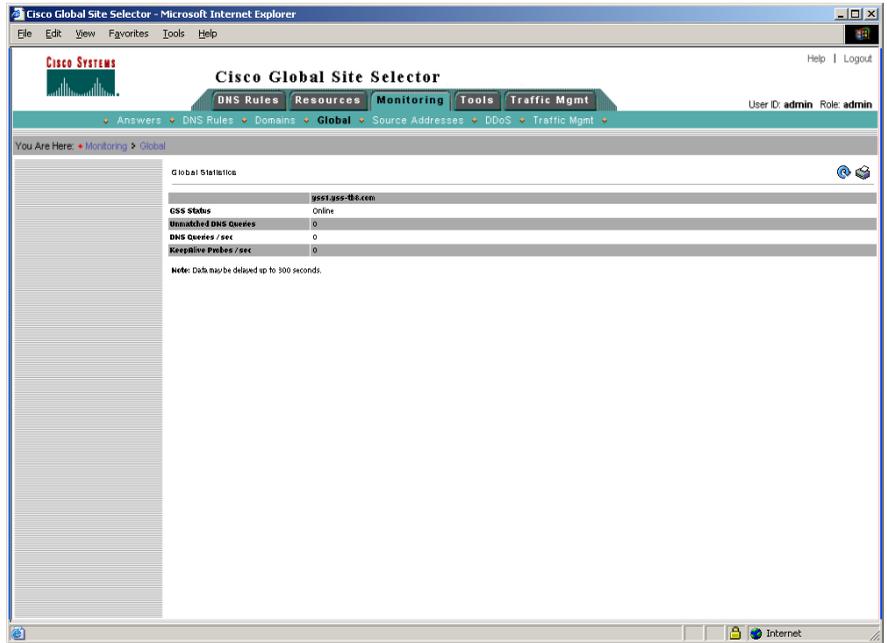


Table 13-60 describes the fields on the Global Statistics list page.

Table 13-60 Field Descriptions for Global Statistics List Page

Field	Description
GSS Status	Online status of each GSS device in your GSS network.
Unmatched DNS Queries	Total number of DNS queries received by each listed device for which no answer could be found.
DNS Queries/sec	Average number of DNS queries received, per second, by each listed GSS device.
Keepalive Probes/sec	Average number of keepalive probes received by each listed GSS device each second.

- Click the column header of any of the displayed columns to sort the listed domains by a particular property.

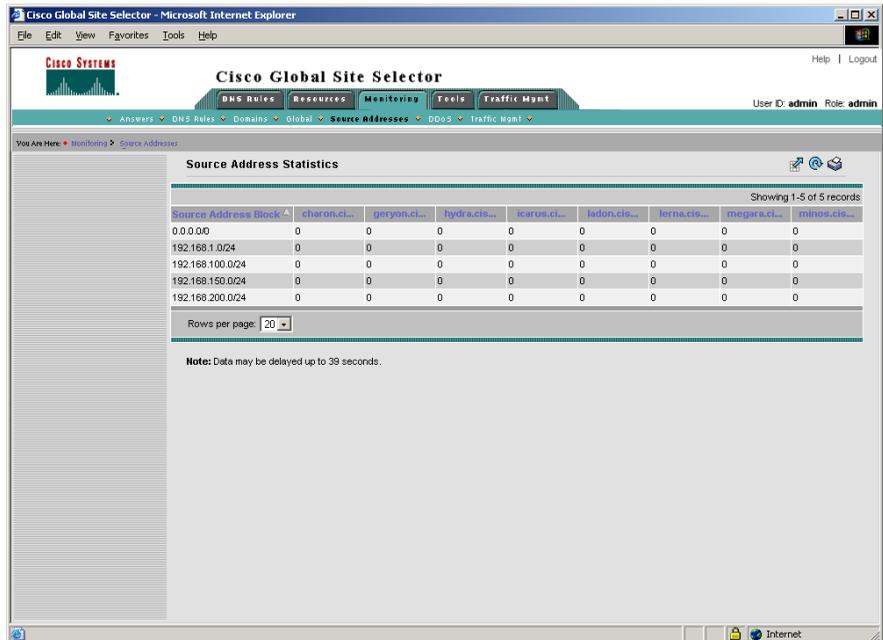
Displaying Source Address Statistics

The Source Address Statistics list page displays statistics about the incoming requests received from each source address (the addresses that transmit DNS queries to a GSS). The source address hit counts feature tracks requests from individual address blocks, not from GSS source address lists, which may contain one or more address blocks.

To display the statistics for your source address lists, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Source Addresses** navigation link. The Source Address Statistics list page appears (see [Figure 13-7](#)).

Figure 13-7 Source Address Statistics List Page



240163

Table 13-61 describes the fields on the Source Address Statistics list page.

Table 13-61 Field Descriptions for Source Address Statistics List Page

Field	Description
Source Address Block	Address or range of addresses that originate the DNS queries. Source address blocks make up GSS source address lists.
Name of the GSS or GSSM	Total number of requests received by the listed GSS device from each source address or address block.

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

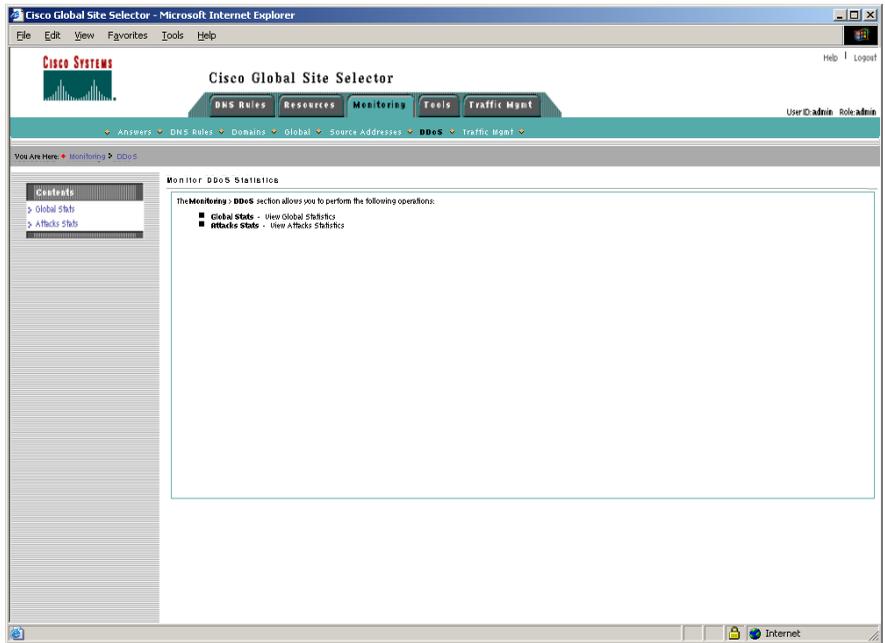
Displaying DDoS Statistics

The Monitor DDoS Statistics page displays selections that allow you to view DDoS global or attack statistics for each GSS in the network.

To display DDoS statistics, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **DDoS** navigation link. The Monitor DDoS Statistics page appears with two sub-menu items, Global Stats and Attack Stats (see [Figure 13-8](#)).

Figure 13-8 Monitor DDoS Statistics Menu Page



3. Click the **Global Stats** selection to view the DDoS Global Statistics (see [Figure 13-9](#)).

Figure 13-9 DDoS Global Statistics List Page

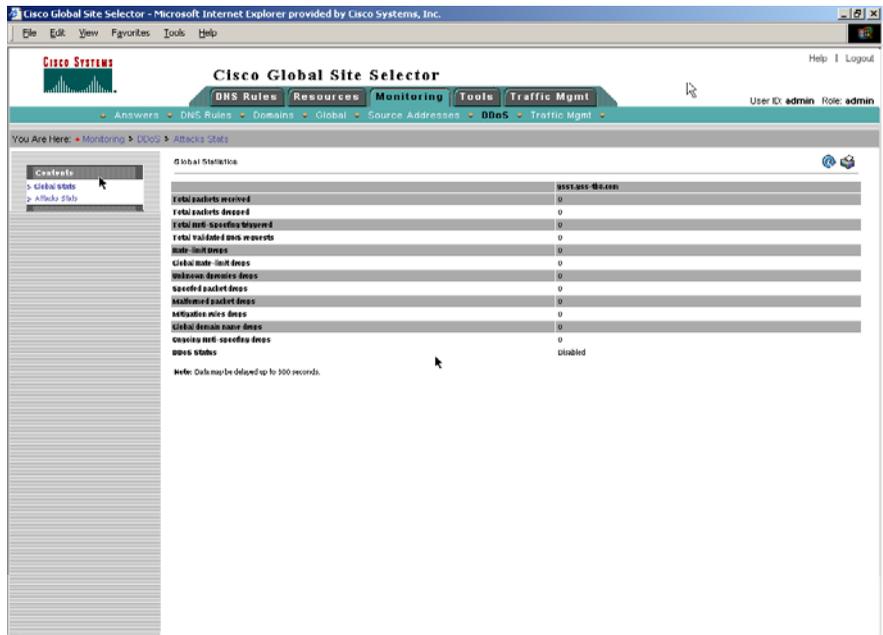


Table 13-62 describes the fields on the Global Statistics list page.

Table 13-62 Field Descriptions for Global Statistics List Page

Field	Description
Total packets received	Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.
Total packets dropped	Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.
Total Anti-Spoofing triggered	Total number of packets that triggered the GSS DDoS protection anti-spoofing function.
Total Validated DNS requests	Total number of packets that were successfully dropped by the GSS DDoS protection anti-spoofing function.

Table 13-62 Field Descriptions for Global Statistics List Page

Field	Description
Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation rate-limiting functions as part of an attack and dropped. The rate limit is the maximum number of DNS requests the GSS can receive from the D-proxy per second.
Global Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.
Unknown dproxies drops	An D-proxy that has not been classified as spoofed or non-spoofed by the DDoS protection and mitigation function is unknown. The DDoS function starts anti-spoofing for an unknown D-proxy. If the number of packets from unknown D-Proxies exceeds the specified rate limit, the unknown drops start.
Spoofed packet drops	Packets that were identified by the GSS DDoS protection and mitigation unknown D-proxy functions as part of an attack and dropped.
Malformed packet drops	Packets that were identified by the GSS DDoS protection and mitigation functions malformed and dropped.
Mitigation rules drops	Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.
Global domain name drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.
Ongoing anti-spoofing drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.
DDoS Status	DDoS detection and mitigation module status, enabled or disabled.

- Click the **Attack Stats** selection to view the DDoS Attack Statistics (see Figure 13-10).

Figure 13-10 DDoS Attack Statistics List Page

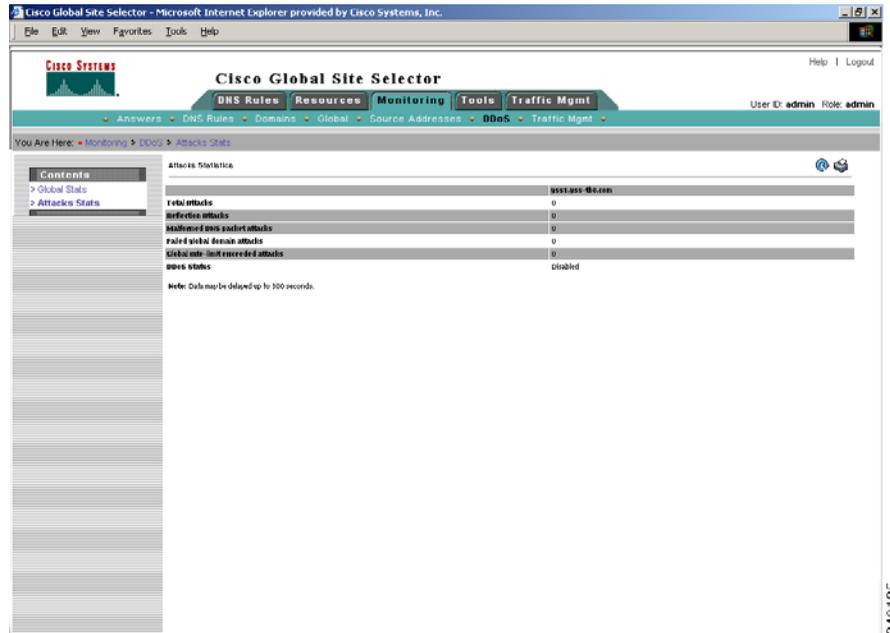


Table 13-63 describes the fields on the Attack Statistics list page.

Table 13-63 Field Descriptions for Attack Statistics List Page

Field	Description
Reflection attacks	Attack in which the IP address of the victim (that is, the GSS) is spoofed and multiple DNS requests are sent to a DNS server or multiple DNS servers posing as the victim.
Malformed DNS packet attacks	Attack in which the GSS is flooded with malformed DNS packets.
Failed global domain attacks	Failed domain counter provides a total for DNS queries that failed to match the global domain name.

Table 13-63 Field Descriptions for Attack Statistics List Page

Field	Description
Global rate-limit exceeded attacks	Attack in which the maximum number of DNS requests that the GSS receives from the D-proxy per second exceeds the global limit.
DDoS status	DDoS detection and mitigation module status, enabled or disabled.

Monitoring Traffic Management Statistics

The Traffic Mgmt section of the Monitoring tab displays global statistics about network proximity and DNS sticky operation in your GSS network. Network proximity statistics include information about the proximity DNS rule hit counts, statistics about the number of entries in the proximity database of each GSS device, and statistics about probing requests. Sticky statistics include information about the sticky DNS rule hit counts and statistics about the number of entries in the sticky database of each GSS device.

This section contains the following topics:

- [Displaying Proximity Rule Hit Count Statistics](#)
- [Displaying Proximity Database Statistics](#)
- [Displaying Proximity Lookup Statistics](#)
- [Displaying Proximity Probe Management Statistics](#)
- [Displaying Sticky Rule Hit Statistics](#)
- [Displaying Sticky Database Statistics](#)
- [Displaying Global Sticky Mesh Statistics](#)

Displaying Proximity Rule Hit Count Statistics

The Proximity Rule Hit Count Statistics list page displays statistics about how many times a DNS rule provides an answer for a zone determined to be the most proximate.

To display statistics about proximity hits for a DNS rule, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Proximity Rule Hit Counts** navigation link (located in the Contents list). The Proximity Rule Hit Statistics list page appears (see Figure 13-11).

Figure 13-11 Proximity Rule Hit Statistics List Page

The screenshot shows the Cisco Global Site Selector GUI. The main content area is titled "Proximity Rule Hit Statistics" and displays a table with the following data:

Name	Owner	gos-superstar.cisco.com	naragump.gos.cisco.com
ProxRule	System	3	0

Below the table, there is a "Rows per page:" dropdown menu set to 20. A legend box on the right side of the page contains the following text:

- Proximity rule total hits
- Proximity rule successful hits

A note at the bottom of the page states: "Note: Data may be delayed up to 300 seconds."

Table 13-64 describes the fields on the Proximity Rule Hit Statistics list page.

Table 13-64 Field Descriptions for Proximity Rule Hit Statistics List Page

Field	Description
Name	Name of the matched DNS rule.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	<p>For each GSS or GSSM, lists the following:</p> <ul style="list-style-type: none"> • Number of DNS requests that match the DNS rule. • Number of DNS responses successfully returned with a proximate answer for the DNS rule. <p>Refer to the legend that appears below the listed DNS rules for information about identifying which value represents the proximity hit count and which value represents the number of successful matches.</p>

Displaying Proximity Database Statistics

The Proximity Database Statistics list page displays statistics about the number of entries in the proximity database and the number of entries dropped because the proximity database reached the maximum database limit of 500,000 entries.

To display the number of entries in the proximity database, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Proximity Database Stats** navigation link (located in the Contents list). The Proximity Database Statistics list page appears (see [Figure 13-12](#)).

Figure 13-12 Proximity Database Statistics List Page

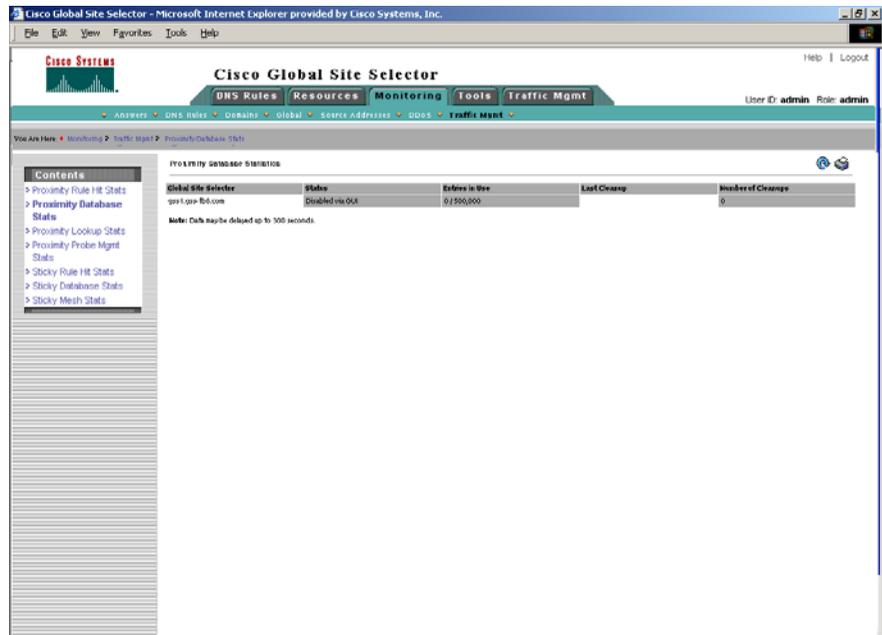


Table 13-65 describes the fields on the Proximity Database Statistics list page.

Table 13-65 Field Descriptions for Proximity Database Statistics List Page

Field	Description
Global Site Selector	Name of the GSS or GSSM device.
Entries in Use	Number of entries currently in the proximity database, out of a maximum of 500,000 entries.
Last Cleanup	Last time that the GSS removed the least recently used entries from the proximity database.
Number of Cleanups	Number of entries removed during the cleanup process.

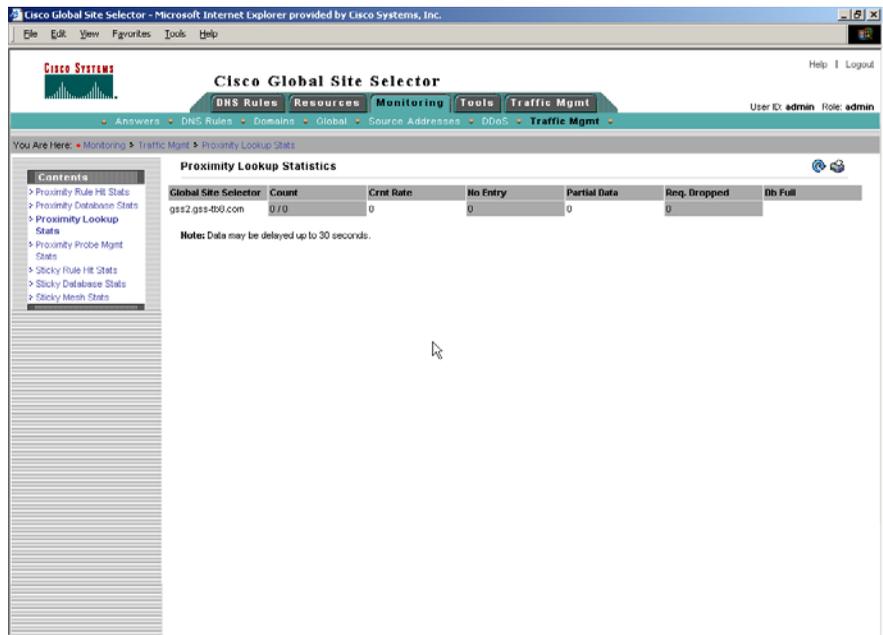
Displaying Proximity Lookup Statistics

The Proximity Lookup Statistics list page displays statistics about the number of entries in the proximity database.

To display the lookup statistics in the proximity database, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Proximity Lookup Stats** navigation link (located in the Contents list). The Proximity Lookup Statistics list page appears (see [Figure 13-13](#)).

Figure 13-13 Proximity Lookup Statistics List Page



240156

Table 13-66 describes the fields on the Proximity Lookup Statistics list page.

Table 13-66 Field Descriptions for Proximity Lookup Statistics List Page

Field	Description
Global Site Selector	Name of the GSS or GSSM device.
Count	Total number of proximity lookup requests made to the GSS.
Crnt Rate	Current request rate per second that requests are made to the GSS to perform a proximity lookup in the database.
No Entry	Number of times that the GSS was unable to locate a proximate answer from the proximity database.
Partial Data	Number of times that only round-trip time (RTT) data for a partial set of zones was available in the proximity database.
Req. Dropped	Number of proximity lookup queries dropped by the GSS.
Db Full	Number of times that the GSS was unable to perform a proximity add because the database exceeded the maximum number of entries.

Displaying Proximity Probe Management Statistics

The Proximity Probe Management Statistics list page displays statistics about the ICMP and TCP probes transmitted from the probing devices.

To display statistics about the probing requests and responses, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Proximity Probe Mgmt Stats** navigation link (located in the Contents list). The Proximity Probe Mgmt Statistics list page appears (see [Figure 13-14](#)).

Figure 13-14 Proximity Probe Mgmt Statistics List Page

The screenshot shows the Cisco Global Site Selector GUI. The main content area is titled "Proximity Probe Mgmt Statistics" and displays a table with 4 records. The table has columns for Zone Index, Zone Name, and two columns of traffic statistics for different probe devices. A legend in the bottom right corner explains the traffic types: Probe Device, Sent Packets, Received Packets, and Current Rate.

Zone Index	Zone Name	gss-superstar.cisco.com	narayang.gss.cisco.com
7	england	10.86.191.158(p) 4,713 2,747 1	10.86.191.158(p) 44 44 0
1	india	10.86.209.162(p) 4,203 4,199 0	10.86.209.162(p) 83 0 0
5	japan	10.86.209.163(p) 4,204 4,200 0	10.86.209.163(p) 44 44 0
3	NewEngland	192.168.10.67(p) 5,605 0 0	192.168.10.67(p) 63 0 0
		192.168.10.68(b) 5,605 0 0	192.168.10.68(b) 83 0 0

Rows per page: 20

Legend:
 Probe Device
 Sent Packets
 Received Packets
 Current Rate

240158

Table 13-67 describes the fields on the Proximity Probe Mgmt Statistics list page.

Table 13-67 Field Descriptions for Proximity Probe Mgmt Statistics List Page

Field	Description
Zone Index	Numerical identifier of the proximity zone.
Zone Name	Name of the proximity zone.
Name of the GSS or GSSM	<p>For each GSS or GSSM, lists the following:</p> <ul style="list-style-type: none"> • IP address of the probe device. • Total number of DRP echo and measurement packets sent by the GSS to the probing device in the proximity zone. • Total number of DRP echo and measurement packets received by the GSS from the probing device in the proximity zone. • Current packet send rate per second. <p>Refer to the legend that appears below the listed zones for information about identifying which value represents sent echo and measurement packets, which value represents received echo and measurement packets, and which value represents the current packet send rate.</p>

Displaying Sticky Rule Hit Statistics

The Sticky Rule Hit Statistics list page displays how many times the GSS accesses a DNS rule and makes a best effort to provide identical A-record responses to the requesting client D-proxy.

To display statistics about sticky hits for a DNS rule, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Sticky Rule Stats** navigation link (located in the Contents list). The Sticky Rule Hit Statistics list page appears (see [Figure 13-15](#)).

Figure 13-15 Sticky Rule Hit Statistics List Page

The screenshot shows the Cisco Global Site Selector GUI. The main content area displays a table of Sticky Rule Hit Statistics. The table has 11 columns: System, and ten numerical columns. The rows represent different DNS rules. A 'Contents' sidebar on the left lists various navigation options. A 'Legend' box at the bottom right indicates that the numerical values represent 'Sticky rule hits' and 'Sticky rule misses'. A note at the bottom states 'Notes: Data may be delayed up to 30 seconds.'

System	130	924	521	45	1,027	1,629	0	141	2,500
alpha3	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
double	130	924	521	45	1,027	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
double1	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
double2	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
double3	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
quad	130	924	520	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,214	2,500	2,500	1,105	1,409	2,500	
quad1	130	924	520	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,214	2,500	2,500	1,105	1,409	2,500	
quad2	130	924	520	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,214	2,500	2,500	1,105	1,409	2,500	
quad3	171	924	546	45	1,025	1,629	13	150	2,491
	2,467	2,500	2,188	2,500	2,500	1,105	1,396	2,491	
triple	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
triple1	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
triple2	130	924	521	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,213	2,500	2,500	1,105	1,409	2,500	
triple3	130	924	520	45	1,026	1,629	0	141	2,500
	2,500	2,500	2,214	2,500	2,500	1,105	1,409	2,500	

240166

Table 13-68 describes the fields on the Sticky Rule Hit Statistics list page.

Table 13-68 Field Descriptions for Sticky Rule Hit Statistics List Page

Field	Description
Name	Name of the matched DNS rule.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	<p>For each GSS or GSSM, lists the following:</p> <ul style="list-style-type: none"> Total number of successful sticky answer matches in the sticky database for the DNS rule. Total number of failed sticky answer lookups in the sticky database for the DNS rule. <p>Refer to the legend that appears below the listed DNS rules for information about identifying which value represents successful matches and which value represents failed lookups.</p>

Displaying Sticky Database Statistics

The Sticky Database Statistics list page displays the number of entries in the sticky database.

To display the number of entries in the sticky database, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Sticky Database Stats** navigation link (located in the Contents list). The Sticky Database Statistics list page appears (see [Figure 13-16](#)).

Figure 13-16 Sticky Database Statistics List Page

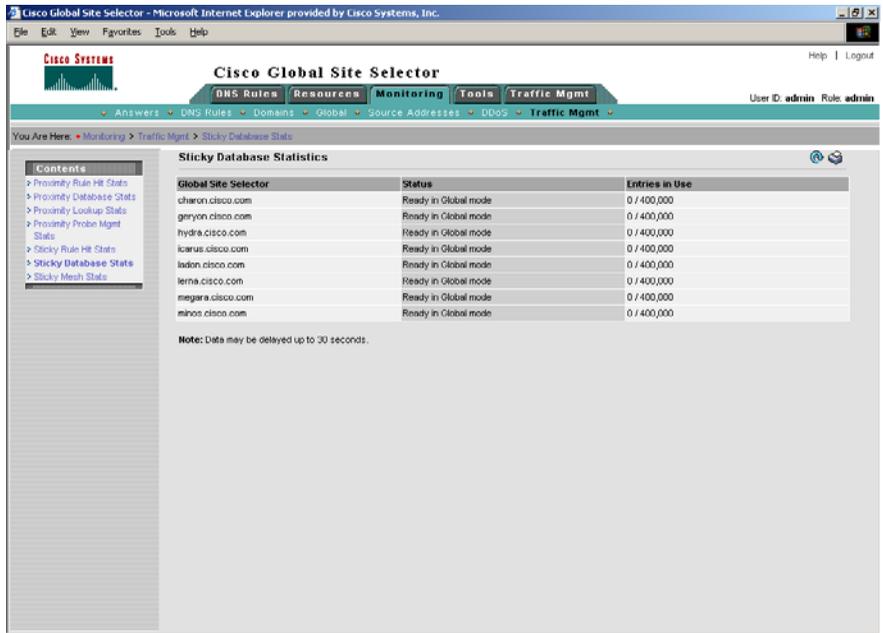


Table 13-69 describes the fields on the Sticky Database Statistics list page.

Table 13-69 Field Descriptions for Sticky Database Statistics List Page

Field	Description
Global Site Selector	Name of the GSS device (GSSM or GSS).
Status	Sticky status of the named device and sticky mode. Status conditions can include Disabled, Local, Global, and Stopped.
Entries in Use	Number of entries currently in the sticky database out of a maximum of 400,000 entries.

Displaying Global Sticky Mesh Statistics

The Sticky Mesh Statistics list page displays the global mesh statistics for all GSS devices in the mesh. This list page identifies all of the GSS devices in the mesh in an X by Y matrix, with each cell displaying the device online status, packets received, packets sent, and any connection down events encountered between the nodes. The statistics appear from the local GSS node's view (X) of the session to each mesh peer (Y).

To display the global mesh statistics, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Traffic Mgmt** navigation link.
3. Click the **Sticky Mesh Stats** navigation link (located in the Contents list).
The Sticky Mesh Statistics list page appears (see [Figure 13-17](#)).

Figure 13-17 Sticky Mesh Stats List Page

The screenshot shows the Cisco Global Site Selector GUI. The navigation tabs include DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. The current page is 'Sticky Mesh Stats'. A 'Contents' sidebar on the left lists various monitoring options, with 'Sticky Mesh Stats' selected. The main area displays a table of statistics for several GSS devices.

Device	geryon.cis...	hydra.cis...	icarus.cis...	ladon.cis...	lerna.cis...	megara.cis...	minos.cis...
geryon.cis...	Up 329 210 0	- 347 0	Up 402 347 0	Up 325 200 0	Up 402 419 0	Up 401 304 0	Up 185 101 307 0
hydra.cis...	Up 413 310 0	Up 347 402 0	- 326 288 0	Up 402 419 0	Up 361 512 0	Up 303 181 0	Up 337 305 0
icarus.cis...	Up 209 481 0	Up 200 325 0	Up 200 326 0	- 325 325 0	Up 200 200 0	Up 196 181 0	Up 200 206 0
ladon.cis...	Up 332 211 0	Up 419 402 0	Up 419 402 0	Up 325 200 0	- 535 307 0	Up 185 180 0	Up 331 306 0
lerna.cis...	Up 338 310 0	Up 394 401 0	Up 512 381 0	Up 326 288 0	Up 367 535 0	- 187 181 0	Up 338 306 0
megara.cis...	Up 180 185 0	Up 191 185 0	Up 101 303 0	Up 101 186 0	Up 100 185 0	Up 167 167 0	Up 180 185 0
minos.cis...	Up 308 310 0	Up 307 401 0	Up 305 337 0	Up 288 280 0	Up 306 321 0	Up 306 320 0	Up 185 100 0

Legend:
 Connection to peer status
 Packets transmitted
 Packets received
 Errors

Note: Data may be delayed up to 30 seconds.

Table 13-70 describes the fields on the Sticky Mesh Statistics list page.

Table 13-70 Field Descriptions for Sticky Mesh Statistics List Page

Field	Description
GSS/Peer	Name of the GSS device (GSSM or GSS) in the mesh along with its peers.
Name of the GSS or GSSM in the mesh	<p>For each GSS peer in the mesh, each column lists the following statistics:</p> <ul style="list-style-type: none"> • Connection to peer status—Online status of each peer in the mesh. The possible states are Stopped, Init, Opened, Authentication, Up, and Down. • Packets transmitted—Number of packets transmitted from the GSS or GSSM to each peer in the mesh. • Packets received—Number of packets received by the GSS or GSSM from each peer in the mesh. • Down Events—The number of down events encountered for the session between the peers in the mesh. <p>Refer to the legend that appears below the listed peer GSS or GSSM in the mesh for information about identifying which statistic represents the online peer status, packets transmitted, packets received, and session down events.</p>



Primary GSSM Global Server Load-Balancing Error Messages

This appendix describes error messages that you may encounter when using the primary GSSM GUI to perform global server load balancing. Error messages are organized by primary GSSM GUI components.

This chapter contains the following major sections:

- [Answer Error Messages](#)
- [Answer Group Error Messages](#)
- [Domain List Error Messages](#)
- [DNS Rule Error Messages](#)
- [KeepAlive Error Messages](#)
- [Location Error Messages](#)
- [Network Error Messages](#)
- [Owner Error Messages](#)
- [Proximity Error Messages](#)
- [Region Error Messages](#)
- [Source Address List Error Messages](#)
- [Sticky Error Messages](#)
- [User Account Error Messages](#)
- [User Views Error Messages](#)

Answer Error Messages

Table A-1 lists the potential error messages that may appear when configuring answers.

Table A-1 Answer Error Messages

Error Message	Description	Recommended Action
Invalid answer name. If entered, name must not be the empty string.	You entered an invalid name for the answer. Answer names cannot be blank or contain blank spaces.	Enter a valid alphanumeric answer name between 1 and 80 characters that does not contain spaces.
Invalid answer name. Name length must not exceed 80 characters.	You entered an answer name that contains too many characters.	Enter a valid alphanumeric answer name between 1 and 80 characters that does not contain spaces.
Invalid CRA timing decay. Timing decay must be between 1 and 10.	You entered an invalid number for the CRA timing decay.	Enter a number between 1 and 10. Lower timing decay values mean that more recent DNS races are weighted more heavily than older races. Higher decay values mean that the results of older races are weighted more heavily than more recent races.
Invalid CRA static RTT value. Static RTT must be between 0 and 1000.	You entered an invalid number for the static round-trip time (RTT). This manually entered value is used by the GSS to represent the time it takes for traffic to reach and return from a host.	Enter a static RTT value between 0 and 1000.
A <i>VIP/Name Server/CRA-type</i> answer named <i>answer_name</i> already exists. If specified, name and type must uniquely identify an answer.	You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and answer type.	Assign a new name or answer type to your answer to make it unique.

Table A-1 Answer Error Messages (continued)

Error Message	Description	Recommended Action
An unnamed <i>VIP/Name Server/CRA</i> -type answer having address <i>IP_address</i> already exists. Name must be specified to configure an answer with the same address as another answer.	You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and IP address.	Assign a new name to your answer to make it unique.
The maximum number of <i>number VIP/Name Server/CRA</i> -type answers has been met.	You attempted to create an answer when the maximum number of that type of answer has already been created.	Remove an existing answer of the same type.
CRA decay value must be specified.	You attempted to create a CRA answer type without specifying a decay value. The decay value is required to tell the GSS how to evaluate and weigh DNS race results.	Enter a number between 1 and 10 for the CRA decay, with 1 causing the GSS to weigh recent DNS race results more heavily, and 10 telling it to weigh them less heavily.
CRA static RTT must be specified.	You attempted to create a CRA answer type without specifying a static round-trip time (RTT) value. The RTT value is used to force the GSS to use a value that you supply as the round-trip time necessary to reach the requesting D-proxy.	Enter a number between 1 and 1000 for the CRA round-trip time in milliseconds.
Invalid keepalive tag. Tag must be at least one character in length.	You attempted to create a VIP answer with a KAL-AP By Tag keepalive, but you have not specified a value for the tag in the field provided.	Enter an alphanumeric tag between 1 and 76 characters in the Tag field.
Invalid keepalive tag. Tag length must not exceed 76 characters.	You attempted to create a VIP answer with a KAL-AP By Tag keepalive, but you have specified a value for the tag that contains too many characters.	Enter an alphanumeric tag between 1 and 76 characters in the Tag field.

Answer Group Error Messages

Table A-1 Answer Error Messages (continued)

Error Message	Description	Recommended Action
NS-type answer <i>IP Address</i> has the same IP address as GSS <i>GSS_name</i> . GSS IP addresses must not equal any NS-type answers.	You attempted to create a name server answer type with the same IP address as a GSS device on the same GSS network. Name server answers cannot use the same address as GSS devices belonging to the same GSS network.	Assign a valid IP address to your name server answer.
Invalid answer order. Order must not be negative.	You attempted to assign a negative order number to your answer. The order must be a positive number.	Enter a nonnegative whole number for the order.

Answer Group Error Messages

Table A-2 lists the potential error messages that may appear when configuring answer groups.

Table A-2 Answer Group Error Messages

Error Message	Description	Recommended Action
This answer group cannot be deleted because it is referenced by <i>number</i> DNS rule balance clause(s).	You attempted to delete an answer group that is being referenced by one or more DNS rules.	Modify any DNS rules that are referencing the answer group so that those rules do not point to the group, and then try again to delete the group.
Invalid answer group name. Name must be entered.	You attempted to create an answer group without assigning a name to that group. All answer groups must have names of at least one character.	Enter a name for the new answer group in the field provided, and then click Save .

Table A-2 Answer Group Error Messages (continued)

Error Message	Description	Recommended Action
Invalid answer group name. Name length must not exceed 80 characters.	You attempted to assign an invalid name to the answer group.	Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
Invalid answer group name. Name must not contain spaces.	You attempted to assign an invalid name to the answer group.	Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
An answer group named <i>name</i> already exists. Name must uniquely identify an answer group.	You attempted to assign the answer group a name that is already being used by a different GSS device.	Enter a unique alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
The maximum number of <i>number</i> answers per <i>VIP/Name Server/CRA</i> -type group has been met.	You attempted to add an answer to an answer group to which the maximum number of answers has already been assigned.	Remove an answer from the group, or add the answer to a group to which the maximum number of answers has not already been added.
Invalid answer load threshold. Load threshold must be between 2 and 254.	You attempted to assign an invalid load threshold to your answer in the LT field.	Assign a load threshold for the answer that is between 2 and 254 in the LT field.

Domain List Error Messages

Table A-3 lists the potential error messages that may appear when configuring domain lists.

Table A-3 Domain List Error Messages

Error Message	Description	Recommended Action
<code><domain name> must contain at least one character.</code>	You attempted to add a domain to a domain list with an invalid name. Domains in domain lists must have names of at least one character.	Enter a name that is between 1 and 100 characters and then save your domain list.
<code><domain name> character limit exceeded.</code>	You attempted to add a domain to a domain list using a name that is too long. Domains in domain lists cannot have names with more than 100 characters.	Enter a new domain name of no more than 100 characters and then save your domain list.
<code>Domain specification must not exceed 128 characters.</code>	You attempted to add a domain to your domain list with a name that is longer than 128 characters. Domain lists cannot contain domains with names that have more than 128 characters.	Replace the domain with a domain name containing fewer than 128 characters and then save your domain list.
<code><domain name> must not contain spaces.</code>	You attempted to add a domain to your domain list with a name that contains spaces. Domains in domain lists cannot have names that contain spaces.	Modify the domain name so that it does not contain spaces and then save your domain list.
<code><domain name> is not a valid regular expression: <regular expression syntax error message here></code>	You attempted to add a domain name to a domain list with a name that contains invalid characters or formatting. Domain names in domain lists must be valid regular expressions.	Modify the domain name so that it is a valid regular expression and does not contain any invalid characters or formatting (for example, <code>www.cisco.com</code> or <code>.*\cisco\.com</code>), and then save your domain list.

Table A-3 Domain List Error Messages (continued)

Error Message	Description	Recommended Action
<domain name> must not begin or end with '.'	You attempted to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of the domain name.	Modify the domain name so that it does not contain a period at the beginning or end of the name and then save your domain list.
<domain name> component must not begin or end with '-'	You attempted to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of one component of the domain name (for example, www.cisco-.com).	Modify the domain name so that it does not contain a dash (-) at the beginning or end of any segment of the name and then save your domain list.
<domain name> contains invalid character '<character>' (<ASCII value of the character>)	You attempted to add a domain to a domain list with a name that contains an invalid text character. Domains belonging to domain lists must have names that are regular expressions.	Modify the domain name so that it does not contain an invalid text character and then save your domain list.
This domain list cannot be deleted because it is referenced by X DNS rule	You attempted to delete a domain list that is being referenced by one or more DNS rules.	Modify any DNS rules that use the domain list so that they no longer reference it and then try again to delete the list.
Invalid domain list name. Name must be entered.	You attempted to create a domain list without a name. Domain lists must have names of at least one character.	Assign a name that has between 1 and 80 characters to your domain list and then save it.
Invalid domain list name. Name length must not exceed 80 characters.	You attempted to create a domain list with a name that is too long.	Assign a name that has between 1 and 80 characters to your domain list and then save it.

Domain List Error Messages
Table A-3 Domain List Error Messages (continued)

Error Message	Description	Recommended Action
Invalid domain list name. Name must not contain spaces.	You attempted to create a domain list with a name that contains spaces. Domain list names cannot contain spaces.	Assign a name without spaces to your domain list. Names must consist of between 1 and 80 characters. Save your domain list when you have assigned it a valid name.
A domain list named '<name>' already exists. Name must uniquely identify a domain list.	You attempted to assign a name to your domain list that has already been assigned to another domain list on the same GSS network.	Assign a unique name to your new domain list and then save the list.
The maximum number of <limit> domains per list has been met.	You attempted to add a domain to your domain list when the maximum number of domains has already been added to that list.	Remove an existing domain from the domain list and then add the new domain. Alternatively, create a domain list to hold the new domain and any subsequent domains that you want to add.

DNS Rule Error Messages

Table A-4 lists the potential error messages that may appear when configuring DNS rules.

Table A-4 DNS Rules Error Messages

Error Message	Description	Recommended Action
TTL must be specified for balance method associated with CRA- or VIP-type answer group.	You attempted to create a balance clause without specifying a Time To Live (TTL) for answers returned by the clause.	Enter a TTL value between 0 and 604,800 seconds.
Invalid balance clause TTL. TTL must be between 0 and 604,800.	You attempted to create a balance clause with an incorrect TTL value for answers provided by the balance clause.	Enter a TTL value between 0 and 604,800 seconds.
Invalid balance clause position. Position must be between 0 and 2.	You attempted to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.	Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order with no gaps between them.
Hash type must be specified for answer group using hash balance method.	You attempted to create an answer group using the balance method “Hashed” with the selected answer, but you have not selected one (or more) hash methods: By Domain Name and By Source Address.	Select one or more of the available hash methods by checking the box corresponding to the methods that you want to use with this balance clause.

DNS Rule Error Messages

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
Balance clause boomerang fragment size must be specified.	You attempted to create a balance clause using the boomerang balance method but have not specified a fragment size in the Fragment Size field. The fragment size determines the preferred size of the boomerang race response that is produced by a match to a DNS rule and is sent to the requesting client.	Enter a fragment size between 28 and 1980 in the field provided. The fragment size must be divisible by 4.
Invalid balance clause Boomerang fragment size. Boomerang fragment size must be 0 or between 28 and 1980.	You attempted to specify an unacceptable fragment size for this balance clause in the Fragment Size field.	Enter a valid fragment size. Fragment sizes must be between 28 and 1980 and must be divisible by 4.
Invalid balance clause Boomerang fragment size. Boomerang fragment size must be a multiple of 4.	You attempted to specify a fragment for this boomerang balance clause that is within the acceptable range but not divisible by 4. Fragment sizes must be divisible by 4.	Enter a fragment size between 28 and 1980 that is also divisible by 4. Zero is also an acceptable fragment size.
Balance clause Boomerang IP TTL value must be specified.	You attempted to create a balance clause using the boomerang balance method but have not specified an IP Time To Live (TTL) in the field provided. The IP TTL specifies the maximum number of network hops that can be used when returning a response to a CRA from a match on a DNS rule.	Enter an IP TTL between 1 and 255 in the field provided and then click Save .
Invalid balance clause Boomerang IP TTL. Boomerang IP TTL must be between 1 and 255.	You attempted to create a balance clause using the boomerang balance method but have specified an invalid IP Time to Live (TTL).	Enter an IP TTL between 1 and 255 in the field provided and then click Save .

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
Balance clause Boomerang maximum propagation delay must be specified.	You attempted to create a balance clause using the boomerang balance method but have not specified a maximum propagation delay (Max Prop. Delay) in the field provided. The maximum propagation delay specifies the maximum length of time (in milliseconds) before the GSS forwards a Domain Name System (DNS) request to a content routing agent (CRA).	Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.
Invalid balance clause Boomerang maximum propagation delay. Boomerang maximum propagation delay must be between 1 and 1000.	You attempted to create a balance clause using the boomerang balance method but have not specified a valid maximum propagation delay (Max Prop. Delay) in the field provided.	Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.
Balance clause Boomerang padding size must be specified.	You attempted to create a balance clause using the boomerang balance method but have not specified a pad size in the Pad Size field. The pad size is the amount of extra data (in bytes) included with each content routing agent (CRA) response packet and is used to evaluate CRA bandwidth and latency when routing decisions are made.	Enter a valid pad size between 0 and 2000 in the Pad Size field.
Invalid balance clause Boomerang padding size. Boomerang padding size must be between 0 and 2000.	You attempted to create a balance clause using the boomerang balance method but have specified an invalid pad size in the Pad Size field.	Enter a valid pad size between 0 and 2000 in the Pad Size field.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
Invalid balance clause Boomerang secret. If specified, Boomerang secret must be between 1 and 64 characters in length.	You attempted to create a balance clause using the boomerang balance method but have specified an invalid secret in the Secret field. The boomerang secret is a text string between 1 and 64 characters that is used to encrypt critical data sent between the boomerang server and content routing agents (CRAs). This key must be the same for each configured CRA.	Enter a valid boomerang secret between 1 and 64 characters in the Secret field.
Balance clause Boomerang server delay must be specified.	You attempted to create a balance clause using the boomerang balance method but have not specified a server delay in the Server Delay field. The boomerang server delay is the maximum delay (in milliseconds) before the boomerang server component of the GSS forwards the address of its “last gasp” server as a response to the requesting name server.	Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.
Invalid balance clause Boomerang server delay. Boomerang server delay must be between 32 and 999.	You attempted to create a balance clause using the boomerang balance method but have specified an invalid server delay in the Server Delay field.	Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.
Invalid DNS rule name. Name must be entered.	You attempted to create a DNS rule without assigning a name to the rule. DNS rules must have names between 1 and 100 characters.	Assign a name to your DNS rule using the Rule Name field and then try again to save the rule.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
Invalid DNS rule name. Name length must not exceed 100 characters.	You attempted to assign a name to your DNS rule that is too long. The maximum length for DNS rules is 100 characters.	Enter a name for your DNS rule that is between 1 and 100 characters and then attempt to save the rule again.
Invalid DNS rule name. Name must not contain spaces.	You attempted to assign your DNS rule a name that contains spaces.	Enter a valid name for your DNS rule that is between 1 and 100 characters and does not contain spaces.
A DNS rule using the specified source address list, domain list, and matching query type already exists. Source address list, domain list, and matching query type must uniquely identify a DNS rule.	You attempted to create a DNS rule that already exists. DNS rules must specify a unique combination of a source address list, a domain list, and a matching query type.	Reconfigure your DNS rule so that it does not exactly match the preexisting rule and then save the rule.
Duplicate answer group/balance method assignment detected. A DNS rule cannot use the same answer group and balance method in multiple balance clauses.	You attempted to create two identical answer group and balance method clauses in your DNS rule. Each clause must use a unique combination of answer groups and balance methods.	Modify one of your answer group and balance method pairs so that it is no longer identical to the other and then save your DNS rule.
Balance clause gap detected at position {0,1,2}. Balance clauses must be specified sequentially without gaps.	You attempted to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.	Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order with no gaps between them.

DNS Rule Error Messages

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
A DNS rule named <i>DNS_Rule_name</i> already exists. Name must uniquely identify a DNS rule.	You attempted to assign a name to the DNS rule that is already assigned to another rule. DNS rule names must be unique.	Assign a rule to the name that is not already being used and then save the rule.
Balance clause 1/2 cannot be sticky because clause number 0/1 is not sticky.	You attempted to enable sticky on Balance Clause 2 without first enabling sticky on Balance Clause 1. The GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.	Enable sticky for Balance Clause 1 before enabling sticky for Balance Clause 2. If necessary, enable sticky for Balance Clause 2 before enabling sticky for Balance Clause 3.
Invalid balance method. Proximity can not be enabled for balance method Hashed.	You attempted to specify the hashed balance method for an answer group in a balance clause that has proximity enabled. The GSS does not support proximity in a DNS rule with the hashed balance method.	Choose a different balance method for the answer group from the Select Balance Method drop-down list.

KeepAlive Error Messages

Table A-5 lists the potential error messages that may appear when configuring keepalives.

Table A-5 *Keepalive Error Messages*

Error Message	Description	Recommended Action
Invalid CAPP hash secret. Secret must be entered.	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have not specified a secret in the field provided.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
Invalid CAPP hash secret. Secret length must not exceed 31 characters.	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
Invalid HTTP HEAD response timeout.	You attempted to specify an HTTP HEAD response timeout that is invalid.	Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.
Response timeout must be between 20 and 60 seconds.	You attempted to specify an HTTP HEAD response timeout that is invalid.	Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.
Invalid HTTP HEAD destination port. Destination port must be between 1 and 65,535.	You attempted to specify a port number for HTTP HEAD traffic that is invalid.	In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.

KeepAlive Error Messages

Table A-5 Keepalive Error Messages (continued)

Error Message	Description	Recommended Action
Invalid HTTP HEAD path. Path length must not exceed 256 characters.	You attempted to specify an HTTP HEAD path that is not valid.	Enter a valid path shorter than 256 characters in the HTTP HEAD default path field in the Shared Keepalive details page.
Invalid <keepalive type> minimum probe frequency. Frequency must be between <min> and <max>.	You attempted to specify a minimum probe interval for your keepalive type that is invalid.	Specify an interval (in seconds) within the range specified for that keepalive type in the Shared Keepalive details page. The interval range for the CRA keepalive type is between 1 and 60 seconds. For all other keepalive types, it is between 45 and 255 seconds.
Duplicate keepalive address detected. A keepalive must not be configured to use the same primary and secondary addresses.	You attempted to configure a KAL-AP keepalive that is identical to a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a different primary and secondary address.
Duplicate keepalive primary address '<primaryaddress>' detected. An address can be used by at most one KAL-AP type keepalive.	You attempted to configure a KAL-AP keepalive that uses the same primary IP address as a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a primary IP address that is not already being used by another keepalive.
Duplicate keepalive secondary address '<secondary address>' detected. An address can be used by at most one KAL-AP type keepalive.	You attempted to configure a KAL-AP keepalive that uses the same secondary IP address as a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a secondary IP address that is not already being used by another keepalive.
HEAD Duplicate keepalive detected. An HTTP HEAD keepalive must not use the same address, destination path, host tag, and port as another HTTP HEAD keepalive.	You attempted to configure an HTTP HEAD keepalive that features an identical configuration to that of another HTTP HEAD keepalive on your GSS network.	Configure the HTTP HEAD keepalive to use a unique configuration of address, destination path, host tag, and port.

Table A-5 *Keepalive Error Messages (continued)*

Error Message	Description	Recommended Action
Duplicate keepalive detected. An ICMP keepalive must not use the same address as another ICMP keepalive.	You attempted to configure an ICMP keepalive with an IP address that is identical to that of another ICMP keepalive on your GSS network.	Configure the ICMP to use a unique IP address.
Invalid CAPP hash secret. Secret length must not exceed 31 characters.	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
Invalid HTTP HEAD destination port. If specified, destination port must be between 0 and 65,535.	You attempted to specify a port number for HTTP HEAD traffic that is invalid.	In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.
Invalid HTTP HEAD host tag. Host tag length must not exceed 128 characters.	You attempted to create an HTTP HEAD host tag that is too long.	Enter an HTTP HEAD host tag of no more than 128 characters.

Location Error Messages

Table A-6 lists the potential error messages that may appear when configuring locations.

Table A-6 Locations Error Messages

Error Message	Description	Recommended Action
The location is still being referenced by other objects and cannot be removed.	You attempted to delete a location that has answers or GSS devices associated with it.	Dissociate any answers or GSS devices from the location and then try again to delete it.
There already exists a location named <name> in region <region> with the same name. Please specify a different location name.	You attempted to create a location within this region when another location with the same name already exists.	Change the name of the location so that it is unique for the region.

Network Error Messages

Table A-7 lists the potential error messages that may appear when configuring the primary GSSM network.

Table A-7 Primary GSSM Network Error Messages

Error Message	Description	Recommended Action
Maximum number of GSSMs exceeded. A GSS network can contain at most 2 GSSMs.	You attempted to enable a GSSM when there are already two GSSMs enabled on your GSS network.	If necessary, remove your standby GSSM from your GSS network and then try again to enable the GSSM.
The maximum number of <size> <className> has been met.	You attempted to add a resource to your GSS network when the maximum number of that resource already exists.	Remove an existing resource of the same type and then try again to add the new resource.

Owner Error Messages

Table A-8 lists the potential error messages that may appear when configuring owners.

Table A-8 Owners Error Messages

Error Message	Description	Recommended Action
Invalid owner name. Name must be entered.	You attempted to create an owner without assigning a name to the owner.	Owners must have a unique name. Enter a name for the owner in the field provided and then save the owner.
Invalid owner name. Name length must not exceed 80 characters.	You attempted to assign a name to an owner that is too long.	Assign a name to your owner that is no longer than 80 characters.
An owner named <owner name> already exists. Name must uniquely identify an owner.	You attempted to assign a name to your owner that is already assigned to another owner on your GSS network.	Assign a unique name to your owner.

Proximity Error Messages

Table A-9 lists the potential error messages that may appear when configuring network proximity.

Table A-9 Proximity Error Messages

Error Message	Description	Recommended Action
Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.	You entered an incorrect global subnet mask in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a valid host or network subnet mask. Be sure to enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit count notation (for example, /24).

Proximity Error Messages

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
Invalid Equivalence window. Equivalence window must be between 0 and 100	You entered an incorrect Equivalence Window value in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter an equivalence window value from 0 to 100 percent to specify a percentage value that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. The default value is 20 percent.
Invalid Entry inactivity timeout. Entry inactivity timeout must be between 15 and 10080	You entered an incorrect Entry Inactivity Timeout value in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a value from 15 to 10080 minutes, specified in 5-minute intervals (15, 20, 25, 30, and up to 10080), to configure the maximum time interval that can pass without the GSS receiving a lookup request for a proximity database entry before the GSS removes that entry. The default value is 60 minutes.
Invalid Refresh probe interval. Refresh probe interval must be between 1 and 72	You entered an incorrect Refresh Probe Interval value in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a value from 1 to 72 hours to specify the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. The default value is 8 hours.
Invalid Acceptable RTT. Acceptable RTT must be between 50 and 500	You entered an incorrect acceptable RTT value in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.	Enter an acceptable RTT value from 50 to 500 ms to specify the value that the GSS uses as an acceptable RTT value when determining the most proximate answer. The default value is 100 ms.

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
Invalid Acceptable percentage of available zones. Acceptable percentage of available zones must be between 3 and 100	You entered an incorrect proximity acceptable zone percentage in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.	Enter a percentage of zones from 3 to 100 percent to specify a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The default value is 40 percent.
Invalid DRP key. Key must have an Id.	You attempted to create a DRP key without an ID value in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a key identification number from 0 to 255 to specify the ID value used by the GSS. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
Invalid DRP key. Key must have a string.	You attempted to create a DRP key without a string in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. The first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
Invalid key ID. Key with the ID 'xxx' already exists.	You attempted to create a DRP key that is using an existing DRP key ID.	Specify a DRP key with a different ID in the Creating New DRP Key details page. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The range of key identification numbers is from 0 to 255.

■ Proximity Error Messages

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
Invalid DRP Key Id. DRP Key Id must be between 0 and 255.	You entered an incorrect DRP key ID in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a key identification number from 0 to 255 to specify the ID value used by the GSS. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
Invalid DRP Key String Length. DRP Key String Length must be between 1 and 80.	You entered an incorrect DRP key string in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. The first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
Invalid key String. Key String cannot start with a digit.	You attempted to create a DRP key that begins with a number.	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. The first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
Invalid key String. Key String is limited to alphanumeric characters.	You attempted to create a DRP key with non-supported characters.	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. The first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
The maximum of 32 DRP Key has been met.	The primary GSSM GUI supports a maximum of 32 keys.	If necessary, delete one or more DRP authentication keys from the primary GSSM GUI (see Chapter 9, Configuring Network Proximity).
Invalid Zone Index. Zone Index must be between 1 and 32.	You entered an incorrect proximity zone index in the Creating New Zone details page (Traffic Mgmt tab).	Enter an integer from 1 to 32 for the proximity zone Index. There is no default.
Invalid zone name. Zone with index 'xxx' already has the name 'yyy'.	You attempted to create a proximity zone that is using an existing zone name.	Enter a different description of the proximity zone. Only alphanumeric characters and the underscore (_) character are allowed.
Invalid zone index. Zone with the name 'yyy' already has index 'xxx'.	You attempted to create a proximity zone that is using an existing index.	Enter a different proximity zone index. Enter an integer from 1 to 32. There is no default.
The maximum of 32 Zones has been met.	The primary GSSM GUI supports a maximum of 32 proximity zones.	If necessary, delete one or more proximity zones from the primary GSSM GUI (see Chapter 9, Configuring Network Proximity).
Invalid probe device address. A probe device with address '1.2.3.4' already exists.	You attempted to create a proximity zone that is using an existing IP address.	In the Probe Device field or the Backup Probe Device field of the Creating New Zone details page (depending on which field generated the error message), enter the correct IP address for the probe device servicing this zone.

Region Error Messages

Table A-10 lists the potential error messages that may appear when configuring regions.

Table A-10 Regions Error Messages

Error Message	Description	Recommended Action
The region is still being referenced by other objects and cannot be removed.	You attempted to delete a region that is associated with GSSs on your GSS network.	Disassociate the GSSs from the region and then try again to delete the region.
There already exists a region named <region name>. All region names have to be unique.	You attempted to assign a name to the region that is already being used by another region on your GSS network.	Assign a unique name to your region.

Source Address List Error Messages

Table A-11 lists the potential error messages that may appear when configuring source addresses.

Table A-11 Source Address List Error Messages

Error Message	Description	Recommended Action
Invalid source address block '<block string>'. Address block must specify a host or a network.	You attempted to specify an invalid source address range.	Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.
Invalid source address block '<blockstring>'. Address block must specify a class A, B, or C host or network.	You attempted to specify an invalid source address range.	Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.
Invalid source address list name. Name must be entered.	You attempted to create a source address list without assigning a name to the list.	Enter a name for the source address list in the Name field.

Table A-11 Source Address List Error Messages (continued)

Error Message	Description	Recommended Action
Invalid source address list name. Name length must not exceed 80 characters.	You attempted to create a source address list with a name that is too long.	Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.
Invalid source address list name. Name must not contain spaces.	You attempted to create a source address list with a name that contains spaces. Source address list names cannot contain spaces.	Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.
This source address list cannot be deleted because it is referenced by <number> DNS rules.	You attempted to delete a source address list that is referenced by one or more DNS rules.	Disassociate your DNS rules from the source address list using the DNS Rule Builder or DNS Rule Wizard and then attempt to delete the source address list again.
A source address list named '<name>' already exists. Name must uniquely identify a source address list.	You attempted to create a source address list using a name that is already being used by another source address list on your GSS network.	Assign a unique name to your source address list that is no more than 80 characters and does not contain spaces.
The maximum number of 30 source address blocks per list has been met.	You attempted to add a source address block to the source address list, when the maximum of 30 source address blocks has already been added to the list.	Remove an existing source address block, or create a source address list for the source address block that you wish to add.

Sticky Error Messages

Table A-12 lists the potential error messages that may appear when configuring DNS sticky.

Table A-12 Sticky Error Messages

Error Message	Description	Recommended Action
Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.	You entered an incorrect global subnet mask in the Global Proximity Configuration details page.	Enter a valid host or network subnet mask. Be sure to enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit count notation (for example, /24).
Invalid Sticky inactivity timeout. Sticky inactivity timeout must be between 15 and 10080.	You entered an incorrect Entry Inactivity Timeout value in either the Global Sticky Configuration details page or in the DNS Rules Builder	Enter a value from 15 to 10080 minutes, specified in 5 minute intervals (15, 20, 25, 30, up to 10080), to configure the maximum time interval the maximum time period that an unused answer remains valid in the sticky database. The default value is 60 minutes.

Table A-12 Sticky Error Messages (continued)

Error Message	Description	Recommended Action
Invalid Sticky inactivity timeout. Sticky inactivity timeout must be a multiple of 5.	You entered an incorrect Entry Inactivity Timeout value in either the Global Sticky Configuration details page or in the DNS Rules Builder	Enter a value from 15 to 10080 minutes, specified in 5 minute intervals (15, 20, 25, 30, up to 10080), to configure the maximum time interval the maximum time period that an unused answer remains valid in the sticky database. The default value is 60 minutes.
Invalid encryption string. Its length must not exceed 32 characters.	You entered an incorrect encryption string in the Global Sticky Configuration details page (Traffic Mgmt tab).	Enter an unquoted text string with a maximum of 32 characters and no spaces as the encryption string used to authenticate communication between GSS peers in the mesh to prevent unauthorized device access.

User Account Error Messages

Table A-13 lists the potential error messages that may appear when configuring a user account.

Table A-13 Primary GSSM User Account Error Messages

Error Message	Description	Recommended Action
There already exists a user account named <user name>. All user accounts must have a unique username.	You attempted to create a user account with a name identical to that of an existing account.	Assign your new user account a unique name. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
You cannot delete the account with username 'admin'. This account must exist.	You attempted to delete the administrator user account.	The primary GSSM GUI restricts you from deleting the administrator account. See the <i>Cisco Global Site Selector Administration Guide</i> for details.

User Views Error Messages

Table A-14 lists the potential error messages that may appear when creating a user view.

Table A-14 Primary GSSM User Views Error Messages

Error Message	Description	Recommended Action
This view cannot be deleted because it is referenced by [number] user(s).	You attempted to delete a user view that is assigned to one or more user accounts.	Access the Modifying User details page and change the assigned view to View All. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
Invalid view name. Name must be entered.	You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
Invalid view name. Name length must not exceed 80 characters.	You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
A view named [name] already exists. Name must uniquely identify a view.	You entered a duplicate view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
The maximum number of 500 owners per view has been met.	The primary GSSM GUI supports a maximum of 500 owners in a custom user view.	If necessary, delete one or more owners previously assigned to the custom view. See the <i>Cisco Global Site Selector Administration Guide</i> for details.

Table A-14 Primary GSSM User Views Error Messages (continued)

Error Message	Description	Recommended Action
The maximum number of 1000 locations per view has been met.	The primary GSSM GUI supports a maximum of 1000 locations in a custom user view.	If necessary, delete one or more locations previously assigned to the custom view. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
The maximum number of 100 answers per view has been met.	The primary GSSM GUI supports a maximum of 100 answers in a custom user view.	If necessary, delete one or more answers previously assigned to the custom view. See the <i>Cisco Global Site Selector Administration Guide</i> for details.
The maximum number of 100 keepalives per view has been met.	The primary GSSM GUI supports a maximum of 100 keepalives in a custom user view.	If necessary, delete one or more keepalives previously assigned to the custom view. See the <i>Cisco Global Site Selector Administration Guide</i> for details.



Sticky and Proximity XML Schema Files

The GSS includes two XML schema files that you can use to describe and validate the sticky XML and proximity XML output files. The sticky and proximity schemas consist of a series of elements, subelements, and attributes that appear in the XML output files to determine the appearance of the content in the XML file.

Each schema file, `stickySchema.xsd` and `proximitySchema.xsd`, resides in the `/home` directory upon boot up of a GSS device. The `/home` directory is where each XML output file resides.

This appendix describes how you can use the two XML schema files, included with the GSS, to describe and validate the sticky XML and proximity XML output files.

This chapter contains the following sections:

- [Sticky XML Schema File Contents](#)
- [Proximity XML Schema File Contents](#)

Sticky XML Schema File Contents

The following example identifies the contents of the sticky XML schema, stickySchema.xsd:

```
<xsd:schema xmlns="http://www.cisco.com/gss/sticky"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            targetNamespace="http://www.cisco.com/gss/sticky"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified">

  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Cisco GSS Sticky Database
    </xsd:documentation>
  </xsd:annotation>

  <xsd:element name="Sticky_Database" type="StickyDatabaseType"/>
  <xsd:element name="Header" type="HeaderType"/>
  <xsd:element name="Source_Entries" type="SourceEntriesType"/>
  <xsd:element name="Source_Entry" type="SourceEntryType"/>
  <xsd:element name="Group_Entries" type="GroupEntriesType"/>
  <xsd:element name="Group_Entry" type="GroupEntryType"/>

  <xsd:complexType name="StickyDatabaseType">
    <xsd:sequence>
      <xsd:element ref="Header" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="Source_Entries" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="Source_Entry_Count" type="xsd:integer"
        minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="Group_Entries" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="Group_Entry_Count" type="xsd:integer"
        minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="HeaderType">
    <xsd:sequence>
      <xsd:element name="Version" type="xsd:integer"
        minOccurs="1" maxOccurs="1"/>
      <xsd:element name="Time_Stamp" type="xsd:string"
        minOccurs="1" maxOccurs="1"/>
      <xsd:element name="Entry_Count" type="xsd:integer"
        minOccurs="1" maxOccurs="1"/>
      <xsd:element name="Mask" type="xsd:string"
        minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

```
</xsd:complexType>

<xsd:complexType name="SourceEntriesType">
  <xsd:sequence minOccurs="0" maxOccurs="unbounded">
    <xsd:element ref="Source_Entry" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="GroupEntriesType">
  <xsd:sequence minOccurs="0" maxOccurs="unbounded">
    <xsd:element ref="Group_Entry" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SourceEntryType">
  <xsd:sequence>
    <xsd:element name="IP" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="D" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="R" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="A" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="H" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="T" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="GroupEntryType">
  <xsd:sequence>
    <xsd:choice minOccurs="1" maxOccurs="1">
      <xsd:element name="N" type="xsd:string"
        minOccurs="1" maxOccurs="1"/>
      <xsd:element name="G" type="xsd:integer"
        minOccurs="1" maxOccurs="1"/>
    </xsd:choice>
    <xsd:element name="D" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="R" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="A" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="H" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="T" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```

```

        minOccurs="1" maxOccurs="1" />
    </xsd:sequence>
</xsd:complexType>

</xsd:schema>

```

Proximity XML Schema File Contents

The following example identifies the contents of the proximity XML schema, proximitySchema.xsd:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

    <xsd:annotation>
        <xsd:documentation xml:lang="en">
            Cisco GSS Proximity Database
        </xsd:documentation>
    </xsd:annotation>

    <xsd:element name="ProximityDatabase" type="ProximityDatabaseType" />
    <xsd:element name="Header" type="HeaderType" />
    <xsd:element name="Entry" type="EntryType" />
    <xsd:element name="ProbeTarget" type="ProbeTargetType" />
    <xsd:element name="Zone" type="ZoneType" />

    <xsd:complexType name="ProximityDatabaseType">
        <xsd:sequence>
            <xsd:element ref="Header" minOccurs="1" maxOccurs="1" />
            <xsd:element ref="Entry" minOccurs="0" maxOccurs="unbounded" />
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="HeaderType">
        <xsd:sequence>
            <xsd:element name="Version" type="xsd:integer"
                minOccurs="1" maxOccurs="1" />
            <xsd:element name="Time_Stamp" type="xsd:string"
                minOccurs="1" maxOccurs="1" />
            <xsd:element name="EntryCount" type="xsd:integer"
                minOccurs="1" maxOccurs="1" />
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="EntryType">
        <xsd:sequence>
            <xsd:element name="EntryID" type="xsd:string"

```

```

        minOccurs="1" maxOccurs="1"/>
<xsd:element name="ModificationTimeStamp" type="xsd:integer"
  minOccurs="1" maxOccurs="1"/>
<xsd:element name="Static" type="xsd:string"
  minOccurs="1" maxOccurs="1"/>
<xsd:element name="DirectProbingInProgress" type="xsd:string"
  minOccurs="1" maxOccurs="1"/>
<xsd:element name="HitTimeStamp" type="xsd:integer"
  minOccurs="1" maxOccurs="1"/>
<xsd:element name="HitCount" type="xsd:integer"
  minOccurs="1" maxOccurs="1"/>
<xsd:element ref="ProbeTarget" minOccurs="1" maxOccurs="1"/>
<xsd:element ref="Zone" minOccurs="32" maxOccurs="32"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ProbeTargetType">
  <xsd:sequence>
    <xsd:element name="IP" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Method" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Type" type="xsd:string"
      minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ZoneType">
  <xsd:sequence>
    <xsd:element name="ID" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="RTT" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
    <xsd:element name="RefreshTime" type="xsd:integer"
      minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="StaticType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="true"/>
    <xsd:enumeration value="false"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="MethodType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="TCP"/>
  </xsd:restriction>
</xsd:simpleType>

```

```
<xsd:enumeration value="ICMP" />
<xsd:enumeration value="NotUsed" />
</xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="TypeOfType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="static" />
    <xsd:enumeration value="non-static" />
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ZoneIdType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="32" />
  </xsd:restriction>
</xsd:simpleType>

</xsd:schema>
```



GLOSSARY

A

answer

Network resources that respond to user queries. As with domains and source addresses, answers are configured at the primary GSSM by identifying a resource of a particular type on your GSS network to which queries can be directed and which can provide your user's D-proxy with the address of a valid host to serve their request. The three types of possible Answers on a GSS network are as follows:

- Virtual IPs (VIPs)—IP addresses associated with an SLB like the Cisco CSS, CSM, or other Cisco IOS-compliant SLB
- Name Server—A configured DNS name server on your network
- CRA—Content routing agents associated with the GSS boomerang server

answer group

Customer-defined set of virtual IP address (VIP), name server (NS), or content routing agent (CRA) addresses from which an individual answer is selected and used to reply to a content request. Answers are grouped together as resource pools. The GSS, using one of a number of available balance methods, can choose the most appropriate resource to serve each user request from the answers in an answer group.

B

- balance method** Algorithm for selecting the best server. It is used together with an answer group to make up a clause in a DNS rule. Up to three possible response answer group and balance method clauses are available for each DNS rule.
- boomerang** Server load-balancing component of the GSS that uses calculations of network delay to select the site “closest” to the requesting D-proxy. Closeness is determined by conducting DNS races between content routing agents (CRAs) on each host server. The CRA that replies first to the requesting D-proxy is chosen to reply to the request.

C

- client** Content consumer, such as a web browser or multimedia stream player, that makes Domain Name System (DNS) requests for domains managed by the GSS.
- Cisco Network Registrar (CNR)** When coupled with GSS, it extends the product's capabilities and allows GSS to migrate to the top-level of the DNS hierarchy. This permits GSS to behave like a DNS appliance and simplifies the process of managing and configuring the DNS infrastructure.
- content provider** Customer who deploys content on a Content Delivery Network (CDN) or purchases hosting services from a service provider or web hosting service.
- content router** Machine that routes requests for content through Domain Name System (DNS) records.
- content routing agent (CRA)** Software running on a Content Delivery Network (CDN) or server load-balancing device that provides information to a GSS for making content routing decisions and handles content routing requests from the GSS.
- Content Services Switch (CSS)** Cisco server load-balancing appliance for Layer 4 through Layer 7 content.
- Content Switching Module (CSM)** Server load-balancing component for the Catalyst 6500 series switches.

- CRA (keepalive)** Keepalive type used when the GSS answer you are testing is a content routing agent (CRA) associated with the boomerang server component of your GSS, the CRA keepalive type pings a CRA at an address that you specify, returning the online status of the device.
- customer** Cisco customer purchasing GSS hardware, software, or services. Typically, an Internet service provider (ISP), application service provider (ASP), or enterprise customer.

D

- data center** Collection of centrally located devices (content servers, transaction servers, or web caches).
- Distributed Denial of Service (DDoS)** Type of attack designed to deny legitimate users access to specific computer or network resources. Such attacks send several thousand spoofed DNS requests to a target device. The target then treats these requests as valid and returns the DNS replies to the spoofed recipient (i.e., the victim).
- Since the target is busy replying to the attacks, it drops valid DNS requests from legitimate D-proxies. When the number of requests is in the thousands, the attacks can potentially generate a multi-gigabit flood of DNS replies, thus causing congestion in the network. To combat this, the GSS contains a DDoS detection and prevention module.
- DNS race** Balance method initiated by the Boomerang Server component of the GSS that is designed to balance between 2 and 20 sites. DNS race gives all possible CRA's a fair chance at resolving a DNS request using a "race" between sites.
- DNS rule** Central configuration and routing concept of the GSS that allows specific request balance resources, methods, and options to be applied to source address and domain pairs.
- domain list** One or more hosted domains logically grouped for administrative and routing purposes.

D-proxy Client’s local name server, which makes iterative DNS queries on behalf of a client. A single recursive query from a client may result in many iterative queries from a D-proxy. Also referred to as local domain name server (LDNS).

DRP Director Response Protocol (DRP). The GSS uses DRP to communicate with the probing devices, called DRP agents, in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems. You can use any Cisco router that is capable of supporting the DRP agent software and can measure ICMP echo-based RTT as the probing device in a zone. The GSS communicates with the Cisco IOS-based router using the DRP ICMP echo-based RTT query and response method.

F

fully qualified domain name (FQDN) Domain name that specifies the named node’s absolute location relative to the Domain Name System (DNS) root in the DNS hierarchy.

G

global server load balancing (GSLB) System based on the Content Services Switch that directs clients through the Domain Name System (DNS) to different sites based on load and availability. Two versions of GSLB currently exist:

- Rule-based GSLB
- Zone-based GSLB

Global Site Selector (GSS) Cisco content routing device that intelligently responds to Domain Name System (DNS) queries, selecting the “best” content locations to serve those queries based on DNS rules created by the customer.

Global Site Selector Manager (GSSM) Device that administers a GSS network, storing configuration information and statistics for GSS devices. GSS administrators can use CLI commands or the graphical user interface (GUI) to reconfigure or monitor the performance of their GSS network.

global sticky With global DNS sticky enabled, each GSS device in the network shares answers with the other GSS devices in the network, operating as a peer mesh. The individual GSS devices in the mesh each store the requests from client D-proxies in its own local database. When one GSS device in the mesh receives a query from the client for the same hosted domain or domain list, global sticky enables each GSS in the network to make a best effort attempt to return the same answer to the requesting client. This action is performed regardless of which GSS in the network is selected to answer the first and subsequent requests. The individual GSS devices work together to maintain a global sticky database across the network. Each GSS in the peer mesh receives updates from the other peers and sends local changes to its remote peers.

GSS network Set of Global Site Selectors (GSSs) in a scaled, redundant GSS deployment.

H

hosted domain Domain managed by the GSS. A minimum of two levels is required for delegation (for example, foo.com). Domain wildcards are supported.

Hosted Domain List (HDL) A grouping of one or more domains that are being fronted by the GSS. Domains are grouped for administrative and/or load-balancing purposes.

HTTP HEAD Used when the GSS answer that you are testing is a VIP associated with an SLB device such as a CSS or CSM. The HTTP HEAD keepalive type sends a TCP format HTTP HEAD request to a web server at an address that you specify, returning the online status of the device (in the form of a 200 response) as well as information on the web page status and content size.

I

ICMP Keepalive type used when the GSS answer that you are testing is a VIP associated with a SLB device such as a CSS or CSM. The ICMP keepalive type pings the configured VIP address (or a shared keepalive address). Online status is determined by a response from the targeted address, indicating connectivity to the network.

K

- KAL-AP** Keepalive type used when the GSS answer that you are testing is a VIP associated with a SLB device such as a CSS or CSM. The KAL-AP keepalive type sends a detailed query to both a primary (master) and secondary (backup) VIP address that you specify, returning the online status of each interface as well as information on load for whichever address is acting as the master VIP. Depending on your GSS network configuration, the KAL-AP keepalive can be used to either query a VIP address directly or to query an address by way of an alphanumeric tag (KAL-AP By Tag), which can be particularly useful when you are attempting to determine the online status of a device that is located behind a firewall that is performing Network Address Translation (NAT).
- keepalive (KAL)** Periodic testing of availability and status of a content service through the sending of intermittent queries to a specified address using one of a variety of methods.
- The GSS uses both primary keepalive and secondary keepalive IP addresses.
- See the keepalive method entry.
- keepalive method** Protocol or strategy used to determine whether a device is online. Examples include ICMP, TCP, KAL-AP, HTTP HEAD, and CRA round-trip time.

L

- LDNS** Local Domain Name Server for a client.
- load threshold** Balance method option that is used with the VIP Answer type. Specifies a number between 0 and 255, which is compared to the load number being reported by the answer device. If the answer's load is above the specified threshold, the answer is deemed to be offline and unavailable to serve further requests.

local sticky	With local DNS sticky, the GSS device ensures that subsequent client D-proxy requests to the same domain name will be "stuck" to the same location as during the first request. DNS sticky guarantees that all requests from a client D-proxy to a particular host domain or domain list are given the same answer by the GSS for the duration of a user-configurable sticky inactivity time interval, assuming the answer is still valid. Each GSS dynamically builds and maintains a local sticky database that is based on the answers that the GSS sends to the requesting client D-proxies. If a subsequent request comes from the same client D-proxy, and the answer is valid, the GSS returns the cached answer to the client D-proxy.
location	Grouping for devices with common geographical attributes, used for administrative purposes only, and similar to data center or content site. See the data center entry.

N

name server (NS)	Publicly or privately addressable Domain Name System (DNS) server that resolves DNS names to IP addresses. Name servers are used by the GSS for name server forwarding, in which queries that the GSS cannot resolve are forwarded to a designated name server that can resolve them.
name server forwarding	Although not an official balance method, Name Server Forwarding plays a vital role in server load balancing using the GSS. Used in instances where requests for domains cannot be handled by any of the name servers configured on the GSS network, the Name Server Forwarding feature passes on requests it cannot answer to a configured name server that does know. That name server's response is passed through the GSS so that it appears to have come from that device.
None (keepalive)	If the keepalive is set to None (using the GUI) or if no keepalive is specified for an answer (using the CLI), the GSS assumes that the named answer is always online. Setting the keepalive type to None prevents your GSS from taking online status or load into account when routing requests. However, it enables you to expand the types of devices for which the GSS can perform load balancing, including remote caches, application servers, and SLBs.

NS (keepalive) Keepalive that is used when the GSS answer that you are testing is a Name Server (NS). The NS keepalive type sends a query for a domain you specify to a name server at an address that you provide. The online status is determined by the ability of the name server to resolve the domain to an address.

O

order Balance method configuration option that is used when the balance method for the answer group is set to Ordered List. Answers on the list will be given precedence in responding to requests based upon their position in the list.

ordered list Balance method in which each resource within an answer group is assigned a number, from 1 to X—where X is the number of resources in the group. Each number corresponds to the rank of the device in the group, with devices that have lower numbers ranked above those with higher numbers. Using the rankings, the GSS tries each resource in an order established by the GSS administrator, selecting the first available answer to serve a user request. List members are preferred and tried in order. A member will not be used unless all previous members fail to provide a suitable result. The Ordered List method allows you to manage resources at a single content site, for example, in a standalone deployment, or a redundant deployment in which the standby SLBs remain passive and are not used to serve requests.

origin server Machine that serves original or replicated content provider content.

owner Internal department or resource or external customer associated with a group of GSS resources such as domain lists, answer groups, and so on.

P

PDB Proximity database (PDB) that provides the core intelligence for all proximity-based decisions of a GSS. Proximity lookup occurs when a DNS rule is matched and the associated clause has the proximity option enabled. When the GSS receives a request from a D-proxy and decides that a proximate answer should be provided, the GSS identifies the most proximate answer from the PDB that resides in GSS memory (the answer with the lowest RTT time) and sends the answer to the requesting D-proxy. If the PDB proximity process is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from probing devices in every zone in the proximity network, and puts the results into the PDB in GSS memory. The GSS supports a maximum of 500,000 entries in the PDB.

probing Process of measuring RTT from one probing device (DRP agent) to a requesting D-proxy device. Probe management is the intelligence behind each GSS device's interaction with the probing device in a zone. Within each zone, there must be at least one probing device and, optionally, a backup probing device. If the primary probing device fails, the probes are redirected to the backup device. Once the primary probing device becomes available, probes are redirected back to the primary probing device. The GSS supports two probing methods, direct and refresh probing.

proximity Ability to answer DNS requests with the most proximate answers relative to the requesting D-proxy. Proximity refers to the distance or delay in terms of network topology, not geographical distance, between the requesting client's D-proxy and its answer. To determine the most proximate answer, the GSS communicates with a probing device, a Cisco IOS-based router, located in each proximity zone to gather round-trip time (RTT) metric information measured between the requesting client's D-proxy and the zone. Each GSS directs client requests to an available server with the lowest RTT value.

R

region Grouping of GSS locations with common geographic attributes used to organize GSS resources.

- round-robin** Balance method in which each resource within an answer group is listed, though in no particular order. As requests are received, the GSS cycles through the list of resources, selecting the first available answer from the group. The GSS is able to resolve requests by evenly distributing the load among possible answers at both local and remote content sites. This balance method allows you to balance requests among multiple, active data centers hosting identical content, for example, between SLBs at a primary and active standby site that serves requests.
- RTT** Round-trip time (RTT). The GSS transmits DRP queries to one or more probing devices in the GSS network, instructing the DRP agent in the probing device to probe specific D-proxy IP addresses. Each probing device responds to the query by using a standard protocol, such as ICMP or TCP, to measure the RTT between the DRP agent in the zone and the IP address of the requesting client's D-proxy device. From the RTT values in the PDB, the GSS selects the zone with the smallest RTT value as the most proximate zone containing the answer for the client's D-proxy request.

S

- Scripted keepalivs** Keepalive type used when the GSS answer that you are testing is a VIP associated with a SLB device such as a CSS or CSM. The Scripted keepalive type is used to probe third-party devices and obtain the load information. The Scripted keepalive uses the SNMP get request to fetch the load information from the target device.
- Secure Socket Layer (SSL)** Industry-standard method for protecting and encrypting web communication.
- server load balancer (SLB)** Network device that balances content requests to network resources based on content rules and real-time load and availability data collected from those devices. Server load balancers such as the Cisco Content Services Switch (CSS), the Content Switching Module (CSM), and LocalDirector provide publicly routable virtual IP addresses (VIPs) while front-ending content servers, firewalls, Secure Socket Layer (SSL) terminators, and caches. Third-party SLBs are supported in a GSS network through the use of Internet Message Control Protocol (ICMP), TCP, and HTTP HEAD keepalives.

service provider	Cisco customer that provides infrastructure for a Content Delivery Network (CDN). Also ISP (Internet service provider) and ASP (application service provider).
source address list	List of source IPs or source IP blocks that are logically grouped by the system administrator.
static proximity	Type of request routing in which incoming requests from specified D-proxies are routed to statically defined resources that have been identified as being in proximity to the source D-proxies.
sticky	Process of binding a client, via their D-Proxy, to a specific server for some amount of time in order to allow the client to complete a transaction. Stickiness, also known as persistent answers or answer caching, enables a GSS to remember the DNS response returned for a client D-proxy and to later return that same answer when the client D-proxy makes the same request. When you enable stickiness in a DNS rule, the GSS makes a best effort to provide identical A-record responses to the requesting client D-proxy, assuming that the original VIP continues to be available. This GSS supports local and global sticky operation.
sticky database	Database that provides the core intelligence for all DNS sticky-based decisions made by a GSS, on a local or global level. The GSS collects requests from the client D-proxies and stores these requests in memory as the sticky database. Requests may be the IP address of the client D-proxy or a database ID representing a list of D-proxy IP addresses (configured as a D-proxy group). The sticky database stores each hosted domain that the DNS rule matches, which may be a single hosted domain (including wildcard expressions) or a configured list of hosted domains. These components make up each sticky database key that the GSS uses for the lookup, storage, and persistence of stickiness for DNS responses. The GSS supports a maximum of 400,000 entries in the sticky database.
subscriber	Client or set of clients receiving a certain style of DNS routing. Subscribers often pay for application services from the GSS customer.

T

TCP	TCP keepalive is used when the GSS answer that you are testing is to GSLB devices other than a CSS or CSM. These GSLB remote devices can include web servers, LocalDirectors, WAP gateways, and other devices that can be checked using a TCP keepalive. The TCP keepalive initiates a TCP connection to the remote device by performing the three-way handshake sequence.
Time To Live (TTL)	Length of time that a response is to be cached and considered valid by the requesting D-proxy.
transaction	Series of specific client and server interactions that are logically connected to a single activity, such as viewing a large VoD file or performing a secure financial transaction.

V

Video on Demand (VoD)	Generic term for rich media content, including video, audio, presentations and program executables.
Virtual IP Address (VIP)	Used by server load-balancing (SLB) devices such as the Cisco CSS and CSM to represent content hosted on one or more servers under their control. The use of VIPs requests for content is efficiently routed to the proper host without exposing that device's internal IP addresses to external users. When directed to a VIP by a GSS, the client's D-Proxy next queries the SLB device to a suitable host, and the A-record for that device is returned by the SLB device to the D-Proxy as an answer.

W

Web Cache Control Protocol (WCCP)	Cisco IOS feature for packet interception.
Web Network Services (WebNS)	VxWorks-based operating system and software that runs on the Content Services Switch (CSS).

weight

Balance method used when the balance method for the answer group is set to Round-Robin or Least-Loaded. Specified by a number between 1 and 10, weights indicate the capacity of the Answer to respond to requests as follows:

- When used with a round-robin balance method, the number listed will be used by the GSS to create a ratio of the number of times the answer will be used to respond before trying the next answer on the list.
- When used with the least-loaded balance method, the number listed will be used by the GSS as the divisor in calculating the load number associated with the answer, which is used to create a bias in favor of answers with greater capacity.

weighted round robin

Balance method that is similar to round robin in that the GSS cycles through a list of defined answers, choosing the first available answer based on the defined load threshold, and so on. However, using WRR, an additional weight factor is assigned to each answer, biasing the GSS toward certain servers so they are picked more often.

Z**zone**

Based on the arrangement of devices and network partitioned characteristics, a customer network can be logically partitioned into "zones." A zone can be geographically related to data centers in a continent, a country, or a major city. All devices, such as web servers in a data center, that are located in the same zone have the same proximity value when communicating with other areas of the Internet. You can configure a GSS proximity network with up to 32 zones. Within each zone, an active probing device is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one probing device to a requesting D-proxy device.



INDEX

Symbols

[12-3](#), [12-16](#), [12-18](#)

A

answer

- associating with a proximity-based location [9-23](#)
- configuring [6-1](#)
- CRA-type answer, creating [6-13](#)
- CRA-type answer, overview [1-21](#)
- deleting [6-21](#)
- displaying [13-91](#)
- error messages [A-2](#)
- keepalive [1-22](#)
- keepalive statistics [13-91](#)
- modifying all in location [6-20](#)
- modifying an answer [6-16](#)
- name server-type answer, creating [6-15](#)
- name server-type answer, overview [1-20](#)
- overview [1-19](#), [6-1](#)
- reactivating [6-19](#)
- statistics, displaying [13-5](#)

status [13-94](#)

suspending [6-19](#)

suspending all answers in a location [6-20](#)

VIP-type answer, creating [6-3](#)

VIP-type answer, multi-port [1-30](#)

VIP-type answer, overview [1-20](#)

answer group

- adding answers [6-24](#), [6-25](#), [6-26](#)
- balance method options [1-34](#)
- balance methods [6-22](#)
- creating [6-23](#)
- deleting [6-33](#)
- displaying current members [6-32](#)
- DNS rule [1-16](#), [1-20](#), [6-2](#), [7-4](#)
- error messages [A-4](#)
- load threshold [6-26](#)
- modifying [6-27](#)
- order [6-26](#)
- overview [1-19](#), [6-22](#)
- removing answers [6-25](#), [6-26](#), [6-27](#)
- statistics, displaying [13-6](#)
- suspending [6-30](#), [6-31](#)
- suspending or reactivating all for an owner [6-31](#)

weight [6-26](#)

answer hit counts [13-90](#)

answer keepalive statistics [13-91](#)

Anywhere source address [1-18, 3-1](#)

appliance-based global server load balancing [1-10](#)

A record [7-4](#)

attacks command [13-18](#)

authentication [9-16](#)

B

balance clause [6-22, 7-4, 7-8, 7-10, 7-12, 7-13, 8-12, 8-20, 8-23, 9-13, 9-30, 9-31](#)

balance method

- answer group options [1-34](#)
- answer group pair [6-22](#)
- balance clauses [6-22](#)
- boomerang [1-33](#)
- DNS rule [1-16, 1-20, 6-2, 7-4](#)
- hash [1-33, 7-7, 7-9, 8-24, 9-33](#)
- least loaded [1-32](#)
- ordered list [1-31, 7-6, 7-8, 8-23, 9-32](#)
- order option [1-35](#)
- overview [1-31](#)
- proximity [9-30](#)
- round robin [1-32, 7-6, 7-8, 8-23, 9-32](#)
- sticky [8-21](#)
- weighted round robin [1-32, 7-7, 7-9, 8-24, 9-33](#)
- weight option [1-35](#)

BIND sample zone configuration file [7-18](#)

boomerang

- activity, displaying [13-3](#)
- balance method [1-33](#)
- clear statistics [13-87](#)
- DNS race [1-33](#)
- server [1-34](#)
- server, displaying status [13-3](#)
- server status [13-3](#)

C

Cisco IOS-based router

- DRP agent, configuring [9-15](#)
- IOS release 12.1 interoperability considerations [9-17](#)
- selecting as DRP agent [9-16](#)
- supported releases [9-16](#)

clauses (balance clause) in answer group [6-22](#)

CLI device management [1-46](#)

closeness (DNS race) [6-13](#)

CNR

- See Cisco Network Registrar

communication between nodes [1-44](#)

configuration file

- global server load balancing [11-1](#)
- playing [11-1](#)

Content Services Switch

- data center deployment [1-45](#)
- definition [G-2](#)

- global load-balancing [1-2](#)
- GSS network deployment [1-10](#)
- VIP answers [1-20](#)

Content Switching Module

- data center deployment [1-45](#)
- definition [G-2](#)
- global load-balancing [1-2](#)
- GSS network deployment [1-10](#)
- VIP answers [1-20](#)

CRA

- answer, creating [6-13](#)
- balance method [1-35](#), [6-22](#)
- clear statistics [13-88](#)
- closeness [6-13](#)
- CRA answer overview [1-21](#)
- definition [G-2](#)
- DNS race [6-13](#)
- global keepalive configuration [5-20](#)
- keepalive [1-27](#)
- last gasp address [7-11](#)
- minimum frequency [5-20](#)
- one way delay [6-14](#)
- overview [1-27](#)
- proximity DNS race [6-13](#)
- round-trip time [6-14](#)
- showing statistics [13-28](#)
- timing decay [5-20](#)

CSM

- See Content Switching Module

CSS

- See Content Services Switch

D

data center

- definition [G-3](#)
- deployment [1-45](#)

DDoS

- attacks statistics, clearing [13-87](#)
- attack statistics, displaying [13-18](#)
- clear statistics [13-87](#)
- detection and mitigation
 - affected network areas [1-38](#)
 - anti-spoofing [1-41](#)
 - configuration [1-38](#)
 - filter checking [1-39](#)
 - overview [1-38](#)
 - rate-limiting [1-40](#)
 - types of attacks prevented [1-39](#)
- failed DNS queries, displaying [13-20](#)
- global statistics, clearing [13-87](#)
- global statistics, displaying [13-24](#)
- rate-limits, displaying [13-22](#)
- running configuration, displaying [13-23](#), [13-27](#)
- spoofed/non-spoofed D-proxies, displaying [13-19](#)
- statistics, monitoring [13-101](#)
- show [13-18](#), [13-19](#), [13-20](#), [13-22](#), [13-24](#), [13-27](#)
- delay [6-14](#)

- delegation
 - definition [1-3](#)
 - domains to GSS [1-43, 7-17](#)
 - GSS devices [7-17](#)
 - subdomains to GSS [1-43, 7-17](#)
- deployment
 - configuring name servers [7-17](#)
 - data center [1-45](#)
 - locations and regions [2-2](#)
 - overview [1-42](#)
 - resources [2-2](#)
 - typical GSS deployment [1-42](#)
- displaying
 - answer hit counts [13-90](#)
 - answer keepalive statistics [13-91](#)
 - answer status [13-94](#)
 - DNS rule statistics [13-95](#)
 - domain configuration information [12-5](#)
 - global load-balancing configuration information [12-1](#)
 - global load-balancing status [13-89](#)
 - global statistics [13-101](#)
 - global sticky mesh statistics [13-63, 13-77](#)
 - global sticky messaging statistics [13-58, 13-70, 13-73](#)
 - GSS network status through CLI [13-2](#)
 - hosted domain statistics [13-97](#)
 - location configuration information [12-2](#)
 - owner configuration information [12-2](#)
 - proximity database statistics [13-46, 13-108](#)
 - proximity DNS rule hit count statistics [13-106](#)
 - proximity group configuration [13-53, 13-54](#)
 - proximity group statistics [13-48](#)
 - proximity lookup statistics [13-12, 13-45, 13-49, 13-110](#)
 - proximity probe statistics [13-50, 13-51, 13-111](#)
 - proximity properties information [12-18](#)
 - proximity status [13-53](#)
 - region configuration information [12-3](#)
 - source address statistics [13-98](#)
 - status of GSS devices from the GUI [13-43](#)
 - sticky configuration information [12-16](#)
 - sticky database statistics [13-56, 13-69, 13-115](#)
 - sticky DNS rule hit count statistics [13-114](#)
 - sticky global mesh statistics [13-117](#)
 - sticky group information [12-16](#)
 - sticky group statistics [13-65, 13-66, 13-86](#)
 - sticky lookup statistics [13-16, 13-56](#)
 - sticky properties [12-17](#)
 - sticky status [13-67](#)
 - zone configuration information [12-3](#)
- DistributedDirector
 - configuration file [11-2](#)
 - playing script files [11-2](#)
 - text file [11-2](#)
- DNS
 - all [7-4](#)
 - A record [7-4](#)
 - balance clause [7-4, 7-6, 7-8, 7-10, 7-12, 7-13, 8-12, 8-20, 8-23, 9-13, 9-30, 9-31](#)

- clear statistics [13-87](#)
- creating DNS rules [7-3](#)
- delegation [7-17](#)
- DNS query [7-3, 7-12](#)
- glue A records [7-17](#)
- GSS as an appliance
- GSS role in hierarchy [1-9](#)
- hosted domain [1-18](#)
- iterative request [1-8](#)
- negative response queries [1-5](#)
 - common response codes [1-6](#)
- query [1-18](#)
- race [1-21, 6-13, 7-10, 12-15](#)
- record request [7-4](#)
- recursive request [1-7](#)
- request resolution [1-8](#)
- resource records [1-4](#)
- routing overview [1-3](#)
- sample BIND zone configuration [7-18](#)
- server, displaying [13-4](#)
- server, modifying [7-17](#)
- SOA records [1-4](#)
 - configuring for negative responses [1-7](#)
 - fields [1-5](#)
 - format [1-4](#)
 - TTL [1-6](#)
 - TTL fields [1-5, 1-9](#)
- traditional routing [1-3](#)
- unmatched queries [13-99](#)
 - zone configuration file [7-18](#)
- DNS race
 - balance method [1-33](#)
 - closeness [6-13](#)
 - coordinate start time [6-13](#)
 - CRAAs [1-21, 7-10, 12-15](#)
- DNS rule
 - adding sticky to [8-21](#)
 - answer [1-16, G-2](#)
 - balance clause [6-22](#)
 - components [1-16](#)
 - creating [7-3](#)
 - definition [G-3](#)
 - deleting [7-16](#)
 - displaying [7-14](#)
 - error messages [A-6](#)
 - filters, configuring [7-17](#)
 - hit count [13-95](#)
 - modifying [7-12, 7-13](#)
 - overview [1-15](#)
 - proximity, enabling/disabling [9-25](#)
 - reactivating all by owner [7-15](#)
 - statistics, displaying [13-12](#)
 - sticky, disabling [8-22](#)
 - sticky, enabling/disabling [8-20, 8-23](#)
 - sticky, enabling by domain [8-22](#)
 - sticky, enabling by domain list [8-22](#)
 - sticky overview [8-21](#)
 - sticky timeout [8-22](#)

- suspending [7-14](#)
- DNS sticky
 - See sticky
- documentation
 - audience [xviii](#)
 - caution and note overview [xxii](#)
 - conventions [xx, xxi](#)
 - organization [xviii](#)
 - related [xx](#)
 - set [xx](#)
 - symbols and conventions [xxi](#)
- domain lists
 - adding domains to [4-4](#)
 - creating [4-3](#)
 - deleting [4-4](#)
 - displaying [4-5](#)
 - error messages [A-15](#)
 - maximum domains [1-19](#)
 - maximum nonwildcard domain length [4-4](#)
 - overview [1-19, 4-1](#)
 - regular expressions [4-4](#)
 - statistics, displaying [13-9](#)
 - sticky by domain list [8-22](#)
 - wildcards in domains [4-4](#)
- domain name space [1-3](#)
- Domain Name System
 - See DNS
- domains
 - delegating to GSS [1-43, 7-18](#)
 - displaying configured [12-5](#)
 - hit counts [13-97](#)
 - maximum length [4-4](#)
 - maximum name length [4-4](#)
 - maximum per domain list [1-19, 4-1](#)
 - statistics, displaying [13-8](#)
 - sticky by domain [8-22](#)
 - wildcards maximum length [4-4](#)
- D-proxy
 - background [1-7](#)
 - definition [G-4](#)
 - iterative requests [1-8](#)
 - name server forwarding [1-20](#)
 - query GSS [1-18](#)
- dproxy command [13-19](#)
- DRP
 - authentication, enabling (Cisco IOS router) [9-16](#)
 - authentication, enabling (GSS) [9-12, 9-28, 9-29](#)
 - key chain (Cisco IOS router) [9-16](#)
 - key identification number (GSS) [9-28](#)
 - key number [9-28](#)
 - keys, creating (Cisco IOS router) [9-16](#)
 - keys, creating (GSS) [9-28, 9-29](#)
 - keys, deleting (GSS) [9-30](#)
 - overview [9-3](#)
- DRP agent
 - clear statistics [13-87](#)
 - configuring Cisco IOS-based router [9-15](#)
 - displaying status [13-17](#)

enabling [9-16](#)
 IOS release 12.1 interoperability considerations [9-17](#)
 overview [9-3](#)
 RTT measurement [9-3](#)
 selecting Cisco IOS-based router [9-16](#)
 supported Cisco IOS releases [9-16](#)
 drpagent
 server status [13-17](#)
 drpagent displaying [13-17](#)

E

error messages
 answer [A-2](#)
 answer group [A-4](#)
 DNS rule [A-6](#)
 domain list [A-15](#)
 GSSM [A-24](#)
 location [A-18](#)
 owner [A-19](#)
 proximity [A-19](#)
 region [A-19](#)
 shared keepalive [A-15](#)
 source address list [A-24](#)
 sticky [A-26](#)
 user [A-27](#)
 user view [A-28](#)
 user views [A-28](#)

F

failed-dns command [13-20](#)
 failure detection time, adjusting [1-27](#)
 firewall
 deploying GSS devices [1-43](#)
 permitting traffic to GSS [1-43](#)
 fully qualified domain name [G-4](#), [G-5](#)

G

global keepalives
 CRA configuration settings [5-20](#)
 fast transmission rate [1-27](#)
 HTTP HEAD configuration settings [5-11](#)
 ICMP configuration settings [5-6](#), [5-16](#)
 KAL-AP configuration settings [5-14](#)
 modifying [5-3](#)
 name server configuration settings [5-21](#)
 overview [5-3](#)
 Scripted keepalive configuration settings [5-18](#)
 standard transmission rate [1-27](#)
 TCP configuration settings [5-8](#)
 global server load balancing
 balance clauses [6-22](#)
 configuration file, copying [11-3](#), [11-4](#)
 configuration file, creating [11-3](#)
 configuration file, modifying [11-5](#)
 configuration file, playing [11-7](#)

- configuration file modification
 - guidelines [11-5](#)
 - configuration file overview [11-2](#)
 - configuration files [11-1](#)
 - configuration order [1-47](#)
 - data centers [1-45](#)
 - definition [G-4](#)
 - delegation of GSS devices [7-17](#)
 - displaying [13-89](#)
 - global statistics [13-98](#)
 - overview [1-11](#)
 - playing script files [11-1](#)
 - script play [11-1](#)
 - summary [1-47](#)
 - traffic management overview [1-36](#)
 - using the GSS [1-10](#)
- Global Site Selector
- acting as GSSM [1-14, 1-42](#)
 - authoritative DNS server [1-11](#)
 - balancing data centers [1-45](#)
 - boomerang server [13-3](#)
 - CLI-based management [1-46](#)
 - communication [1-44](#)
 - delegation of devices [7-17](#)
 - deployment [1-42, 1-43, 1-45, 7-17](#)
 - DNS server, displaying [13-4](#)
 - factors in responding to a request [1-11](#)
 - general statistics, displaying [13-10](#)
 - global server load balancing [1-10](#)
 - GSLB configuration [1-47](#)
 - GUI-based management [1-47](#)
 - hardware [1-14](#)
 - interact with SLBs [1-11](#)
 - inter-GSS communications [1-44](#)
 - keepalives overview [1-22, 5-1](#)
 - locating [1-43](#)
 - network management [1-45](#)
 - overview [1-2, 1-14](#)
 - packet filtering [1-43](#)
 - resources, grouping [2-8](#)
 - software architecture [1-13](#)
 - synchronized with GSSM [1-14, 1-44](#)
- Global Site Selector Manager
- communication [1-44](#)
 - database [1-14, 1-44](#)
 - definition [G-4](#)
 - deployment [1-42](#)
 - DNS rules [1-15](#)
 - error messages [A-24](#)
 - GSLB configuration [1-47](#)
 - inter-GSS communication [1-44](#)
 - keepalives overview [5-1](#)
 - locating [1-43](#)
 - overview [1-14](#)
 - primary [1-14](#)
 - redundancy [1-44](#)
 - resources, grouping [2-8](#)
 - standby [1-14](#)
 - standby, as backup [1-42](#)

- standby acting as primary [1-44](#)
- global statistics [13-101, 13-106](#)
- global sticky
 - authentication [8-6](#)
 - by domain, enabling [8-22](#)
 - by domain list, enabling [8-22](#)
 - clearing sticky mesh statistics [13-88](#)
 - encryption [8-6](#)
 - favored peer [8-8](#)
 - joining the mesh [8-8](#)
 - mesh, communicating [8-7](#)
 - mesh conflict resolution [8-7](#)
 - mesh statistics [13-63, 13-77](#)
 - mesh updates [8-5, 8-6](#)
 - messaging statistics [13-58, 13-70, 13-73](#)
 - overview [8-5](#)
 - peer mesh [8-5](#)
 - synchronizing GSS system clock with peers [8-14](#)
- glossary of terms [G-1](#)
- glue A records [7-17](#)
- GSLB
 - See global server load balancing
- GSS
 - See Global Site Selector
- GSSM
 - See Global Site Selector Manager
- GSS network
 - configuration [1-14, 1-44](#)
 - definition [G-5](#)

- deployment [1-42](#)
- displaying through CLI [13-2](#)
- displaying through GUI [13-89](#)
- global statistics [13-98, 13-101, 13-106](#)
- GSLB status [13-89](#)
- management [1-45](#)
- organizing [2-2](#)
- primary GSSM [1-14](#)
- resource grouping [2-8](#)
- GSS role in DNS hierarchy [1-9](#)
- GUI
 - device management [1-46](#)
 - displaying GSS device status [13-43](#)
 - error messages [A-1](#)
- GUI error messages [A-1](#)

H

- hashed balance method [1-33, 7-7, 7-9, 8-24, 9-33](#)
- hosted domain
 - definition [G-5](#)
 - domain names [1-18](#)
 - name examples [1-18](#)
 - overview [1-18, 4-1](#)
 - regular expressions [1-18](#)
 - requested [1-16](#)
 - statistics [13-97](#)
- HTTP HEAD keepalive
 - global keepalive configuration [5-11](#)

- host tag [5-25, 6-8](#)
 - overview [1-25](#)
 - shared keepalive configuration [5-24](#)
 - statistics [13-34](#)
 - VIP answer [6-8](#)
- HTTP Head keepalive
- default path [5-11](#)
 - destination port [5-11](#)
 - termination method [5-11](#)
-
- I**
- ICMP keepalive
- global keepalive configuration [5-6, 5-16](#)
 - overview [1-25](#)
 - shared keepalive configuration [5-23](#)
 - statistics [13-35](#)
 - VIP answer [6-5](#)
- inter-GSS communication [1-44](#)
- iterative requests [1-8](#)
-
- K**
- KAL
- See keepalive
- KAL-AP keepalive
- by tag [6-9](#)
 - by VIP [6-10](#)
 - CAPP hash secret [5-14, 5-15](#)
 - global keepalive configuration [5-14](#)
 - overview [1-26](#)
 - primary and secondary IP addresses [5-25](#)
 - shared keepalive configuration [5-25](#)
 - statistics [13-37](#)
 - VIP answer [6-9](#)
- keepalive [6-11](#)
- clear statistics [13-87](#)
 - cra, clear statistics [13-88](#)
 - CRA overview [1-27](#)
 - CRA statistics, displaying [13-28](#)
 - CRA type [1-27](#)
 - definition [G-6](#)
 - deleting a shared keepalive [5-30](#)
 - error messages [A-15](#)
 - failure detection time, adjusting [1-27](#)
 - fast transmission rate [1-27](#)
 - global properties, modifying [5-3](#)
 - global properties, overview [5-3](#)
 - global statistics, displaying [13-30](#)
 - http-head, clear statistics [13-88](#)
 - HTTP HEAD overview [1-25](#)
 - HTTP HEAD statistics, displaying [13-34](#)
 - ICMP statistics, displaying [13-35](#)
 - ICMP type [1-25](#)
 - kalap, clear statistics [13-88](#)
 - KAL-AP overview [1-26](#)
 - KAL-AP statistics, displaying [13-37](#)
 - keepalive attempts [1-30, 5-26](#)

- multi-port [1-23](#)
 - name server [1-27](#)
 - name server overview [1-27](#)
 - name server statistics, displaying [13-41](#)
 - none [1-27](#)
 - ns, clear statistics [13-88](#)
 - number of retries [1-29, 5-7, 5-9, 5-10, 5-13, 5-15, 5-17, 5-26, 5-30, 6-6, 6-7, 6-8](#)
 - overview [1-22](#)
 - probes [1-30, 5-7, 5-10, 5-13, 5-15, 5-17, 5-26, 6-6, 6-7, 6-9](#)
 - probes per second [13-99](#)
 - scripted-keepalive clear statistics [13-88](#)
 - Scripted keepalive configuration [5-27](#)
 - Scripted keepalive overview [1-26](#)
 - Scripted statistics, displaying [13-38](#)
 - shared keepalive, creating [5-23](#)
 - shared keepalive overview [5-22](#)
 - shared VIP keepalives, overview [5-22](#)
 - standard transmission rate [1-27](#)
 - supported types [1-22](#)
 - TCP connection termination method [5-24, 6-7](#)
 - TCP overview [1-25](#)
 - TCP statistics, displaying [13-42, 13-43](#)
 - transmission interval formula [1-28](#)
 - VIP [1-25, 1-26, 5-22](#)
-
- least loaded
 - balance method [1-32, 7-6, 7-8, 8-23, 9-32](#)
 - overview [1-32, 7-6, 7-8, 8-23, 9-32](#)
 - weight option [1-35](#)
 - local sticky
 - disabling on a GSS [8-34](#)
 - enabling on a GSS [8-34](#)
 - overview [8-2](#)
 - location
 - associating with a proximity zone [9-13, 9-21](#)
 - creating [2-5](#)
 - definition [G-6, G-7](#)
 - deleting [2-6](#)
 - displaying configured [12-2](#)
 - error messages [A-18](#)
 - modify all answers in [6-20](#)
 - modifying [2-5](#)
 - organizing resources [2-8](#)
 - overview [1-16, 2-2](#)
 - suspending all answers [6-20](#)

M

- monitoring
 - global statistics [13-106](#)
 - See displaying

L

- last gasp address [7-11](#)

N

name server

- answer type, creating [6-15](#)
- authoritative [1-9](#)
- authoritative name server (ANS) [1-7](#)
- balance method [6-22](#)
- balance method options [1-35](#)
- balance methods [7-6, 7-8, 8-13, 8-23, 9-32, 12-14, 12-15](#)
- clear statistics [13-88](#)
- client name server (CNS) [1-7](#)
- definition [G-7](#)
- DNS resolvers (DNSR) [1-7](#)
- forwarding [1-20](#)
- intermediate name server (INS) [1-7](#)
- keepalive [1-27](#)
- name server answer overview [1-20](#)
- overview [1-7](#)
- query [6-16](#)
- records, adding to zone configuration file [7-17](#)
- root name servers (RNS) [1-7](#)

name server keepalive

- global keepalive configuration [5-21](#)
- interval min (minimum frequency) [5-21](#)
- overview [1-27](#)
- query domain [5-21](#)
- statistics [13-41](#)

negative DNS response queries [1-5](#)

- common response codes [1-6](#)

- negative DNS responses queries SOA configuration [1-7](#)

network

- deployment [1-42](#)
- locating GSS on [1-43](#)
- network design guidelines for proximity [9-9](#)
- network management [1-45](#)
 - CLI-based [1-46](#)
 - displaying global server load-balancing statistics [13-89](#)
 - GUI-based [1-47](#)

network proximity

- See proximity

node communication [1-44](#)

NTP server

- enabling [8-14, 9-18](#)
- identifying [8-14, 9-18](#)
- synchronizing GSS system clock with peers [8-14, 9-18](#)

- number of retries for keepalive types [1-29, 5-7, 5-10, 5-17, 6-6, 6-7, 6-8](#)

O

- one-way delay [6-14](#)

ordered list

- balance method [1-31, 7-6, 7-8, 8-23, 9-32](#)
- definition [G-8](#)
- overview [1-31](#)

- order option, balance method [1-35](#)
- origin server [G-8](#)
- owner
 - creating [2-7](#)
 - deleting [2-7](#)
 - displaying configured [12-2](#)
 - error messages [A-19](#)
 - organizing resources [2-8](#)
 - overview [1-17, 2-2](#)
 - reactivating all DNS rules [7-15](#)
 - suspending all answer groups for [6-31](#)
 - suspending all DNS rules [7-15](#)

P

PDB

See proximity database

probing device

- assigning to static database entries [9-40](#)
- initial probe method [9-11, 9-26, 12-19](#)
- manually initiating probing [9-47](#)
- probe device overview [9-3](#)
- probe methods [9-4](#)
- probing process [9-4](#)
- refresh-interval [9-26](#)
- RTT results [9-5](#)

proximity

- acceptable-rtt value [9-27](#)
- acceptable-zone value [9-27](#)

- clearing statistics [13-88](#)
- configuring [9-24](#)
- database statistics, displaying [13-46, 13-108](#)
- deleting database entries [9-42](#)
- deleting static entries [9-41](#)
- disabling [9-25](#)
- DNS rule, adding to [9-31](#)
- DNS rule hit count statistics, displaying [13-106](#)
- DNS rule overview [9-30](#)
- DNS rule statistics, displaying [13-12, 13-45](#)
- dumping proximity database entries [9-43, B-1](#)
- enabling [9-25](#)
- equivalence [9-25](#)
- error messages [A-19, A-28](#)
- group configuration, displaying [13-53, 13-54](#)
- group statistics, displaying [13-48](#)
- inactivity timeout [9-6](#)
- initial probe method [9-11, 9-26, 12-19](#)
- loading proximity database entries [9-46](#)
- locally disabling/enabling proximity on a GSS [9-47](#)
- lookup statistics, displaying [13-49, 13-110](#)
- manually initiating probing [9-47](#)
- mask, specifying [9-11, 9-25, 12-19](#)
- network design guidelines [9-9](#)
- network proximity example [9-7](#)
- overview [9-2](#)
- periodic proximity database backup [9-45](#)
- probe management overview [9-3](#)

- probe methods [9-4](#)
- probe statistics, displaying [13-50](#), [13-51](#), [13-111](#)
- proximity database overview [9-5](#)
- proximity group, creating [9-36](#)
- proximity group, playing static proximity configurations [9-37](#)
- proximity group deletion [9-38](#), [9-39](#)
- proximity group overview [9-35](#)
- quick start [9-10](#)
- results of locally disabling on a GSS [9-48](#)
- static database entries, adding [9-39](#)
- statistics, displaying (CLI) [13-45](#)
- statistics, monitoring (GUI) [13-106](#)
- status, displaying (CLI) [13-45](#)
- subsystem statistics, displaying [13-53](#)
- synchronizing GSS system clock with peers [9-18](#)
- XML schema file [B-1](#)
- zone overview [9-2](#)
- zones, associating with a location [9-21](#)
- zones, associating with an answer [9-23](#)
- zones, creating [9-20](#)
- zones, deleting [9-21](#)
- zones, modifying [9-20](#)
- proximity database
 - age-out process [9-6](#)
 - automatic backup [9-43](#)
 - deleting dynamic entries [9-42](#)
 - deleting static entries [9-41](#), [9-42](#)
 - dumping entries [9-43](#)
 - inactivity timeout [9-6](#)
 - loading entries [9-46](#)
 - maximum number of entries [9-6](#)
 - overview [9-5](#)
 - periodic backup [9-45](#)
 - RTT, assigning to static entries [9-40](#)
 - RTT values [9-5](#)
 - specifying entry format to dump [9-44](#), [B-1](#)
 - static entries, adding [9-39](#)
- proximity group
 - benefits [9-35](#)
 - creating [9-36](#)
 - deleting [9-39](#)
 - entering multiple groups [9-37](#)
 - IP address block, deleting [9-38](#)
 - overview [9-35](#)
 - playing static proximity configurations [9-37](#)
- proximity properties
 - displaying [12-18](#)
- proximity zone
 - acceptable-zone value [9-27](#)
 - associating with an answer [9-23](#)
 - creating [9-20](#)
 - deleting [9-21](#)
 - determining most proximate answer [9-6](#)
 - equivalence [9-25](#)
 - modifying [9-20](#)
 - network design guidelines [9-9](#)
 - overview [9-2](#)

probe methods [9-4](#)
 RTT [9-2](#)
 proximity
 wait enable [9-28](#)

Q

query
 answers [6-2](#)
 balance methods [1-31](#)
 CRA answer [6-13](#)
 DNS request [1-9](#)
 DNS rules [1-15](#)
 KAL-AP [1-26, 6-9](#)
 match DNS query type [7-3](#)
 name server [1-27](#)
 name server answer [6-15](#)
 not matched to D-proxy [1-18](#)
 query domain [5-21](#)
 source addresses [1-17](#)

R

rate-limit command [13-22](#)
 reactivating
 all answer groups for an owner [6-31, 7-15](#)
 all answers in an answer group [6-31](#)
 all answers in location [6-20](#)
 all DNS rules [7-14](#)

 answer [6-19](#)
 DNS rule [7-15](#)
 record request [7-4](#)
 redundancy synchronization [1-44](#)
 refresh-interval [9-26](#)
 region
 creating [2-4](#)
 definition [6-9](#)
 deleting [2-6](#)
 displaying configured [12-3](#)
 error messages [A-19](#)
 organizing resources [2-8](#)
 overview [1-16, 2-2](#)
 regular expressions [1-18, 4-4](#)
 report
 answer hit counts [13-90](#)
 answer status [13-94](#)
 DNS rule hit count [13-95](#)
 domain hit count [13-97](#)
 keepalive statistics [13-91](#)
 source address hit count [13-100](#)
 requests
 iterative [1-8](#)
 resolution [1-7, 1-11](#)
 resource records [1-4](#)
 resources
 configuring [2-1](#)
 grouping [2-8](#)
 organizing [2-2](#)

round robin

- balance method [1-32, 7-6, 7-8, 8-23, 9-32](#)
- overview [1-32](#)

round-trip time (RTT)

- acceptable-rtt value [9-27](#)
- acceptable-zone value [9-27](#)
- assigning to static entries [9-40](#)
- DRP agent [9-3](#)
- equivalence [9-25](#)
- overview [9-2](#)
- probing methods [9-4](#)
- proximity database entries [9-5](#)

RTT

- See round-trip time (RTT)

running-config command [13-27](#)**S**sample BIND zone configuration [7-18](#)

Scripted keepalive

- global keepalive configuration [5-18](#)
- overview [1-26](#)
- shared keepalive configuration [5-26](#)
- statistics [13-38](#)
- VIP answer [6-11](#)

scripted-keepalive

- clear statistics [13-88](#)

script play

- global server load balancing configuration file [11-7](#)

overview [11-2](#)server load balancer [1-2, G-10](#)service provider [G-11](#)ses [12-17](#)

shared keepalive

- creating [5-22](#)
- deleting [5-23, 5-30](#)
- error messages [A-15](#)
- HTTP HEAD configuration settings [5-24](#)
- ICMP configuration settings [5-23](#)
- KAL-AP configuration settings [5-25](#)
- modifying [5-22](#)
- overview [5-22](#)
- Scripted keepalive configuration settings [5-26](#)
- TCP configuration settings [5-23](#)

show ddos-config command [13-23](#)show statistics command [13-2](#)

- boomerang [13-3](#)
- dns [13-4](#)
- dns answer [13-5](#)
- dns answer group [13-6](#)
- dns domain [13-8](#)
- dns domain-list [13-9](#)
- dns global [13-10](#)
- dns proximity rule [13-12, 13-45](#)
- dns rule [13-12](#)
- dns sticky rule [13-16, 13-56](#)
- drpagent [13-17](#)
- keepalive [13-28](#)

- keepalive cra [13-28](#)
- keepalive global [13-30](#)
- keepalive http-head [13-34](#)
- keepalive icmp [13-35](#)
- keepalive kalap [13-37](#)
- keepalive ns [13-41](#)
- keepalive tcp [13-42](#), [13-43](#)
- proximity database [13-46](#)
- proximity group-name [13-48](#)
- proximity group-summary [13-48](#)
- proximity lookup [13-49](#)
- proximity probe [13-50](#), [13-51](#)
- Scripted keepalive [13-38](#)
- source-address [13-14](#)
- source-address-list [13-15](#)
- sticky [13-56](#)
- sticky global [13-58](#)
- sticky group-name [13-66](#)
- sticky group-summary [13-65](#)
- sticky mesh [13-63](#)
- SOA records [1-4](#), [1-5](#), [1-6](#), [1-9](#)
 - configuring for negative responses [1-7](#)
 - format [1-4](#)
 - TTL fields [1-5](#)
- source address
 - Anywhere [1-18](#), [3-1](#)
 - hit counts [13-98](#)
 - maximum per source address list [3-1](#)
 - overview [1-18](#)
 - statistics, displaying [13-14](#)
- source address and domain hash balance
 - method [1-33](#), [7-7](#), [7-9](#), [8-24](#), [9-33](#)
- source address list
 - adding addresses [3-3](#)
 - anywhere [1-18](#)
 - Anywhere (default) [3-1](#)
 - creating [3-1](#)
 - definition [G-11](#)
 - deleting [3-3](#)
 - deleting addresses [3-4](#)
 - error messages [A-24](#)
 - maximum addresses [3-1](#)
 - modifying [3-3](#)
 - overview [1-17](#)
 - statistics, displaying [13-15](#)
- SSL
 - See Secure Socket Layer
- standby GSSM
 - database, synchronized with primary GSSM [1-44](#)
 - definition [1-44](#)
 - overview [1-14](#)
- statistics
 - answer hit counts [13-90](#)
 - answer keepalive [13-91](#)
 - answer status [13-94](#)
 - clearing [13-87](#)
 - clearing DDoS [13-87](#)
 - DNS rule hit count [13-95](#)

- global [13-101](#), [13-106](#)
- hosted domains [13-97](#)
- proximity database [13-108](#)
- proximity DNS rule hit count [13-106](#)
- proximity lookup [13-110](#)
- proximity probe [13-111](#)
- source address [13-98](#)
- sticky database [13-69](#), [13-115](#)
- sticky DNS rule hit count [13-114](#)
- sticky global mesh [13-117](#)
- traffic management, displaying [13-106](#)
- statistics-global command [13-24](#)
- sticky
 - balance clause, enabling for [8-12](#), [8-23](#)
 - by domain, enabling [8-22](#)
 - by domain list, enabling [8-22](#)
 - clearing statistics [13-88](#)
 - configuring [8-16](#)
 - conflict resolution [8-7](#)
 - database entries, deleting [8-28](#)
 - database statistics, displaying [13-56](#), [13-115](#)
 - disabling [8-22](#), [8-34](#)
 - disabling/enabling local sticky on a GSS [8-34](#)
 - displaying configured [12-16](#)
 - DNS rule, adding to [9-31](#)
 - DNS rule hit count statistics, displaying [13-114](#)
 - DNS rule overview [8-21](#)
 - DNS rule statistics, displaying [13-16](#), [13-56](#)
 - dumping sticky database entries [8-30](#), [B-1](#)
 - error messages [A-26](#)
 - global sticky mesh statistics, displaying [13-63](#), [13-77](#)
 - global sticky messaging statistics, displaying [13-58](#), [13-70](#), [13-73](#)
 - global sticky overview [8-5](#)
 - global sticky peer mesh [8-5](#)
 - group statistics, displaying [13-65](#), [13-66](#), [13-86](#)
 - inactivity timeout [8-4](#)
 - loading sticky database entries [8-33](#)
 - local sticky overview [8-2](#)
 - mask, specifying [8-17](#), [8-19](#)
 - mesh favored peer [8-8](#)
 - overview [8-2](#)
 - periodic sticky database backup [8-32](#)
 - quick start guide [8-10](#)
 - results of locally disabling on a GSS [8-34](#)
 - statistics, displaying (CLI) [13-55](#)
 - statistics, displaying (GUI) [13-106](#)
 - status, displaying (CLI) [13-55](#)
 - sticky database overview [8-3](#)
 - sticky global mesh statistics, displaying [13-117](#)
 - sticky group, creating [8-27](#)
 - sticky group, deleting [8-28](#)
 - sticky group overview [8-25](#)
 - subsystem statistics, displaying [13-67](#)
 - timeout [8-11](#), [8-18](#), [8-19](#), [8-22](#), [12-17](#)
 - XML schema file [B-1](#)
- sticky database

- age-out process [8-4](#)
- automatic backup [8-30](#)
- dumping entries [8-30](#)
- loading entries [8-33](#)
- matched entry [8-4](#)
- maximum number of entries [8-4](#)
- overview [8-3](#)
- periodic backup [8-32](#)
- specifying entry format to dump [8-31](#), [B-1](#)
- statistics [13-69](#)
- sticky entries, deleting [8-28](#)
- sticky inactivity timeout [8-4](#)
- sticky timeout [8-11](#), [8-18](#), [8-19](#), [8-22](#), [12-17](#)
- sticky group
 - creating [8-27](#)
 - deleting [8-28](#)
 - displaying information [12-16](#)
 - entering multiple groups [8-27](#)
 - IP address block, deleting [8-28](#)
 - overview [8-25](#)
- sticky properties
 - displaying [12-17](#)
- subdomains, delegation [1-43](#), [7-17](#)
- subscriber [G-11](#)
- suspending
 - all answer groups for an owner [6-31](#)
 - all answers in a location [6-20](#)
 - all answers in an answer group [6-31](#)
 - answer [6-19](#)

- answer group [6-30](#), [6-31](#)
- DNS rule [7-14](#)
- synchronization of primary and standby GSSM [1-44](#)

T

- TCP keepalive
 - global keepalive configuration [5-8](#)
 - overview [1-25](#)
 - port [5-9](#)
 - shared keepalive configuration [5-23](#)
 - statistics [13-42](#), [13-43](#)
 - VIP answer [6-6](#)
- timeout, sticky [8-11](#), [8-18](#), [8-19](#), [12-17](#)
- Time To Live [G-12](#), [G-13](#)
- traffic management
 - load balancing overview [1-36](#)
 - proximity, configuring [9-24](#)
 - proximity overview [1-38](#)
 - proximity zone, configuring [9-20](#)
 - statistics, displaying [13-106](#)
 - sticky, configuring [8-16](#)
 - sticky overview [1-37](#)
- troubleshooting GUI error messages [A-1](#)
- TTL
 - See Time To Live

U

user view error messages [A-28](#)

V
VIP

answer groups [6-22](#)
 answers [6-3](#)
 answer types [6-5](#)
 balance method options [1-34](#)
 balance methods [6-22, 7-6, 7-8, 8-13, 8-23, 9-32, 12-14, 12-15](#)
 http-head, clear statistics [13-88](#)
 icmp, clear statistics [13-88](#)
 kal-ap, clear statistics [13-88](#)
 keepalive type [1-25](#)
 tcp, clear statistics [13-88](#)
 VIP answer overview [1-20](#)

VIP answer

HTTP HEAD keepalive [6-8](#)
 ICMP keepalive [6-5](#)
 KAL-AP keepalive [6-9](#)
 multiple answers and ports, specifying [1-30](#)
 multi-port [1-23, 6-11](#)
 Scripted keepalive [6-11](#)
 TCP keepalive [6-6](#)

VIP answer, creating [6-3](#)
VIP keepalive type

HTTP HEAD [1-25](#)

ICMP [1-25](#)

KAL-AP [1-26](#)

Scripted keepalive [1-26](#)

TCP [1-25](#)

VIP-type answer, multi-port [1-23, 6-11](#)

W
weight

balance method overview [1-35](#)
 least loaded [1-35](#)
 round-robin [1-35](#)

weighted round robin

balance method [1-32, 7-7, 7-9, 8-24, 9-33](#)
 overview [1-32](#)

wildcards

in domains [4-4](#)
 maximum length in domain names [4-4](#)

Z
zone

displaying configured [12-3](#)
 proximity, creating [9-20](#)

zone configuration file (DNS)

modifying [7-17](#)
 sample [7-18](#)