Cisco Global Site Selector
GUI-Based Global Server Load-Balancing Configuration Guide
Software Version 4.1 (1)
November 2011

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
CONTENTS

Preface xiii
Audience xiii
How to Use This Guide xiii
Related Documentation xiv
Symbols and Conventions xv
Obtaining Documentation and Submitting a Service Request xvi

CHAPTER 1

Introducing the Global Site Selector 1-1
GSS Overview 1-2
DNS Routing 1-2
  DNS Name Servers 1-3
  SOA Records 1-4
  Negative Caching 1-4
  SOA Records and Negative Responses 1-5
DNS Structure 1-5
Request Resolution 1-6
Globally Load Balancing with the GSS 1-7
GSS Architecture 1-10
  Global Site Selectors and Global Site Selector Managers 1-10
    Primary GSSM 1-10
    GSS 1-11
    Standby GSSM 1-11
DNS Rules 1-12
Locations and Regions 1-12
Owners 1-13
Source Addresses and Source Address Lists 1-13
Hosted Domains and Domain Lists 1-14
Answers and Answer Groups 1-14
  VIP Answers 1-15
  Name Server Answers 1-15
  CRA Answers 1-16
Keepalives 1-16
  Multiport Keepalives 1-17
ICMP 1-18
TCP 1-19
HTTP HEAD 1-19
HTTPS HEAD 1-19
KAL-AP 1-19
Scripted Keepalive 1-20
CRA 1-20
Name Server 1-20
None 1-20
Adjusting Failure Detection Time for Keepalives 1-21

Balance Methods 1-23
Ordered List Method 1-24
Round-Robin Method 1-24
Weighted Round-Robin Method 1-24
Least-Loaded Method 1-24
Hashed Method 1-25
DNS Race (Boomerang) Method 1-25
Balance Method Options for Answer Groups 1-25

Traffic Management Load Balancing 1-27
DNS Sticky GSLB 1-27
Network Proximity GSLB 1-28
Geo-Location-Based GSLB Feature 1-28

DDoS Detection and Mitigation 1-29
Mitigation Rules 1-30
Rate Limits 1-30
Anti-Spoofing Mechanism 1-31

GSS Network Deployment 1-32
Locating GSS Devices 1-32
Locating GSS Devices Behind Firewalls 1-32
Communication Between GSS Nodes 1-33
Deployment Within Data Centers 1-33

GSS Network Management 1-34
CLI-Based GSS Management 1-34
GUI-Based Primary GSSM Management 1-34

Understanding the Primary GSSM GUI 1-35
GUI Organization 1-36
List Pages 1-36
Details Pages 1-36
Navigation 1-37
Primary GSSM GUI Icons and Symbols 1-37
### Contents

- Primary GSSM GUI Online Help 1-39
- Global Server Load-Balancing Summary 1-40
- Where to Go Next 1-41

#### CHAPTER 2

**Configuring Resources** 2-1
- Organizing Your GSS Network 2-2
- Creating and Modifying Locations and Regions 2-2
  - Creating Regions 2-2
  - Modifying Regions 2-3
  - Add or Modify Regions and States 2-3
  - Creating Locations 2-4
  - Modifying Locations 2-5
  - Deleting Locations and Regions 2-5
- Creating and Modifying Owners 2-6
  - Creating Owners 2-6
  - Modifying Owners 2-6
  - Deleting Owners 2-7
- Grouping GSS Resources by Location, Region, and Owner 2-7
- Managing Global Manual Reactivation of Answers and Clauses 2-8
  - Enabling or Disabling the Global Manual Reactivation Function 2-9
  - Activating All Operationally Suspended Answers or Clauses 2-9
- Where to Go Next 2-9

#### CHAPTER 3

**Configuring Source Address Lists** 3-1
- Creating Source Address Lists 3-2
- Modifying Source Address Lists 3-3
- Deleting Source Address Lists 3-3
- Where to Go Next 3-4

#### CHAPTER 4

**Configuring Domain Lists** 4-1
- Creating Domain Lists 4-1
- Modifying Domain Lists 4-2
- Deleting Domain Lists 4-3
- Where to Go Next 4-3

#### CHAPTER 5

**Configuring Keepalives** 5-1
- Modifying Global Keepalive Properties 5-1
Globally Enabling or Disabling Keepalives 5-2
Modifying ICMP Global Keepalive Settings 5-2

Modifying TCP Global Keepalive Settings 5-3
  Modifying HTTP HEAD Global Keepalive Settings 5-4
  Modifying HTTPS HEAD Global Keepalive Settings 5-6
  Modifying KAL-AP Global Keepalive Settings 5-7
  Modifying Scripted Keepalive Global Keepalive Settings 5-8
  Modifying CRA Global Keepalive Settings 5-8
  Modifying Name Server Global Keepalive Settings 5-9

Configuring and Modifying Shared VIP Keepalives 5-9
  Creating a Shared VIP Keepalive 5-9
    Configuring ICMP Shared Keepalive Configuration Settings 5-10
    Configuring TCP Shared Keepalive Configuration Settings 5-11
    Configuring HTTP HEAD Shared Keepalive Configuration Settings 5-12
    Configuring HTTPS HEAD Shared Keepalive Configuration Settings 5-13
    Configuring KAL-AP Shared Keepalive Configuration Settings 5-14
    Configuring Scripted Keepalive Shared Keepalive Configuration Settings 5-15
  Modifying a Shared Keepalive 5-17
  Deleting a Shared Keepalive 5-17

Where to Go Next 5-18

CHAPTER 6
Configuring Answers and Answer Groups 6-1

Configuring and Modifying Answers 6-1
  Creating a VIP-Type Answer 6-2
    Configuring ICMP Keepalive VIP Answer Settings 6-5
    Configuring TCP Keepalive VIP Answer Settings 6-6
    Configuring HTTP HEAD Keepalive VIP Answer Settings 6-7
    Configuring HTTPS HEAD Keepalive VIP Answer Settings 6-8
    Configuring KAL-AP Keepalive VIP Answer Settings 6-9
    Configuring Scripted Keepalive VIP Answer Settings 6-9
  Creating a CRA-Type Answer 6-10
  Creating a Name Server-Type Answer 6-11

Modifying an Answer 6-12
  Suspending an Answer 6-12
  Reactivating an Answer 6-13
  Suspending or Reactivating All Answers in a Location 6-13
  Deleting an Answer 6-14

Configuring and Modifying Answer Groups 6-14
  Creating an Answer Group 6-15
Building and Modifying DNS Rules 7-1

DNS Rule Configuration Overview 7-2
-- DNS Rule Wizard 7-2
-- DNS Rule Builder 7-2

Building DNS Rules Using the Wizard 7-3
-- Identifying a Source Address List in the DNS Rule Wizard 7-4
-- Specifying a Domain List in the DNS Rule Wizard 7-4
-- Configuring an Answer Group in the DNS Rule Wizard 7-6
-- Choosing a Balance Method in the DNS Rule Wizard 7-8
-- Reviewing the Summary Page in the DNS Rule Wizard 7-9

Building DNS Rules Using the DNS Rule Builder 7-10

Modifying DNS Rules 7-14
-- Suspending a Clause 7-15
-- Reactivating a Clause 7-15

Reactivating Operationally Suspended Clauses 7-15

Suspending a DNS Rule 7-15

Reactivating a DNS Rule 7-16

Suspending or Reactivating All DNS Rules Belonging to an Owner 7-17

Deleting a DNS Rule 7-17

Configuring DNS Rule Filters 7-18

Removing DNS Rule Filters 7-22

Delegating to GSS Devices 7-22

Where To Go Next 7-23
Adding a New GeoDB Static Entry 8-5
Viewing GeoDB Static Entries 8-5
Monitoring GeoDB Statistics 8-6
Monitoring GeoDB Rule Hit Stats 8-6
Monitoring GeoDB Database Stats 8-6
Monitoring GeoDB Lookup Stats 8-7
Where To Go Next 8-7

CHAPTER 9

Configuring DNS Sticky 9-1
DNS Sticky Overview 9-1
Local DNS Sticky 9-2
Sticky Database 9-2
Global DNS Sticky 9-3
  GSS Sticky Peer Mesh 9-4
  Sticky Mesh Conflict Resolution 9-5
  Communicating in the Sticky Peer Mesh 9-5
DNS Sticky Quick Start Guide 9-6
Synchronizing the GSS System Clock with an NTP Server 9-8
Configuring Sticky Using the Primary GSSM GUI 9-9
  Configuring DNS Sticky 9-9
  Configuring the Global Sticky Mesh 9-11
  Enabling Sticky in a DNS Rule 9-12
    Sticky DNS Rule Overview 9-12
    Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups 9-13
Configuring Sticky Using the GSS CLI 9-14
  Logging in to the CLI and Enabling Privileged EXEC Mode 9-14
Creating Sticky Groups 9-15
  DNS Sticky Group Overview 9-15
  Creating a DNS Sticky Group 9-17
  Deleting a Sticky Group IP Address Block 9-17
  Deleting a Sticky Group 9-18
Deleting Entries from the Sticky Database 9-18
Dumping Sticky Database Entries 9-19
Running a Periodic Sticky Database Backup 9-20
Loading Sticky Database Entries 9-20
Disabling DNS Sticky Locally on a GSS for Troubleshooting 9-21
# Chapter 10

## Configuring Network Proximity

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Proximity Overview</td>
<td>10-1</td>
</tr>
<tr>
<td>Proximity Zones</td>
<td>10-2</td>
</tr>
<tr>
<td>Probe Management and Probing</td>
<td>10-2</td>
</tr>
<tr>
<td>Proximity Database</td>
<td>10-4</td>
</tr>
<tr>
<td>Example of Network Proximity</td>
<td>10-5</td>
</tr>
<tr>
<td>Proximity Network Design Guidelines</td>
<td>10-6</td>
</tr>
<tr>
<td>Network Proximity Quick Start Guide</td>
<td>10-7</td>
</tr>
<tr>
<td>Configuring a Cisco Router as a DRP Agent</td>
<td>10-10</td>
</tr>
<tr>
<td>Choosing a Cisco Router as a DRP Agent</td>
<td>10-10</td>
</tr>
<tr>
<td>Configuring the DRP Agent</td>
<td>10-10</td>
</tr>
<tr>
<td>Cisco IOS Release 12.1 Interoperability Considerations</td>
<td>10-11</td>
</tr>
<tr>
<td>Synchronizing the GSS System Clock with an NTP Server</td>
<td>10-11</td>
</tr>
<tr>
<td>Creating Zones Using the Primary GSSM GUI</td>
<td>10-12</td>
</tr>
<tr>
<td>Creating a New Proximity Zone</td>
<td>10-12</td>
</tr>
<tr>
<td>Modifying a Proximity Zone</td>
<td>10-13</td>
</tr>
<tr>
<td>Deleting a Proximity Zone</td>
<td>10-13</td>
</tr>
<tr>
<td>Associating a Proximity Zone with a Location</td>
<td>10-13</td>
</tr>
<tr>
<td>Associating a Proximity-Based Location with an Answer</td>
<td>10-14</td>
</tr>
<tr>
<td>Configuring Proximity Using the Primary GSSM GUI</td>
<td>10-14</td>
</tr>
<tr>
<td>Configuring Proximity</td>
<td>10-14</td>
</tr>
<tr>
<td>Creating DRP Keys</td>
<td>10-17</td>
</tr>
<tr>
<td>Deleting DRP Keys</td>
<td>10-18</td>
</tr>
<tr>
<td>Using the DNS Rule Builder to Add Proximity to a DNS Rule</td>
<td>10-18</td>
</tr>
<tr>
<td>Configuring Proximity Using the GSS CLI</td>
<td>10-20</td>
</tr>
<tr>
<td>Logging in to the CLI and Enabling Privileged EXEC Mode</td>
<td>10-20</td>
</tr>
<tr>
<td>Creating Proximity Groups</td>
<td>10-21</td>
</tr>
<tr>
<td>Proximity Group Overview</td>
<td>10-21</td>
</tr>
<tr>
<td>Creating a Proximity Group</td>
<td>10-22</td>
</tr>
<tr>
<td>Deleting a Proximity Group IP Address Block</td>
<td>10-23</td>
</tr>
<tr>
<td>Deleting a Proximity Group</td>
<td>10-23</td>
</tr>
<tr>
<td>Configuring Static Proximity Database Entries</td>
<td>10-23</td>
</tr>
<tr>
<td>Adding Static Proximity Entries</td>
<td>10-23</td>
</tr>
<tr>
<td>Deleting Static Entries from the Proximity Database</td>
<td>10-25</td>
</tr>
<tr>
<td>Deleting Entries from the Proximity Database</td>
<td>10-25</td>
</tr>
<tr>
<td>Dumping Proximity Database Entries to a File</td>
<td>10-26</td>
</tr>
<tr>
<td>Running a Periodic Proximity Database Backup</td>
<td>10-28</td>
</tr>
<tr>
<td>Loading Proximity Database Entries</td>
<td>10-28</td>
</tr>
</tbody>
</table>
Initiating Probing for a D-Proxy Address 10-29
Disabling Proximity Locally on a GSS for Troubleshooting 10-30
Where to Go Next 10-30

CHAPTER  11
Monitoring GSS Global Server Load-Balancing Operation 11-1
Monitoring Global Server Load-Balancing Statistics from the CLI 11-1
Monitoring the Status of the Boomerang Server on a GSS 11-2
Monitoring the Status of the DNS Server on a GSS 11-2
  Displaying Answer Statistics 11-3
  Displaying Answer Statistics for all GSSs in the GSS Mesh 11-4
  Displaying Answer Group Statistics 11-4
  Displaying Domain Statistics 11-5
  Displaying Domain List Statistics 11-6
  Displaying Global Statistics 11-6
  Displaying DNS Rule Proximity Statistics 11-8
  Displaying DNS Rule Statistics 11-8
  Displaying DNS Rule Statistics for all GSSs in the GSS Mesh 11-9
  Displaying Source Address Statistics 11-10
  Displaying Source Address List Statistics 11-10
  Displaying DNS Rule Sticky Statistics 11-11
Monitoring the Status of the DRP Agent on a GSS 11-11
Monitoring DDoS Statistics on a GSS 11-12
  Displaying DDoS Attack Statistics 11-12
  Displaying DDoS Anti-Spoofing Statistics 11-13
  Displaying DDoS Failed DNS Queries 11-14
  Displaying DDoS Rate-Limit Values 11-15
  Displaying the DDoS Running Configuration 11-16
  Displaying DDoS Statistics 11-17
  Displaying DDoS Status 11-19
Monitoring the Status of Keepalives on a GSS 11-19
  Displaying CRA Keepalive Statistics 11-19
  Displaying Global Keepalive Statistics 11-20
  Displaying HTTP HEAD Keepalive Statistics 11-23
  Displaying HTTPS HEAD Keepalive Statistics 11-24
  Displaying ICMP Keepalive Statistics 11-25
  Displaying KAL-AP Keepalive Statistics 11-26
  Displaying Scripted Keepalive Statistics 11-27
  Displaying Name Server Keepalive Statistics 11-28
  Displaying TCP Keepalive Statistics 11-29
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Network Proximity Statistics on a GSS</td>
<td>11-30</td>
</tr>
<tr>
<td>Displaying DNS Rule Proximity Statistics</td>
<td>11-30</td>
</tr>
<tr>
<td>Displaying Proximity Database Statistics</td>
<td>11-31</td>
</tr>
<tr>
<td>Displaying Proximity Group Statistics</td>
<td>11-32</td>
</tr>
<tr>
<td>Displaying Proximity Lookup Statistics</td>
<td>11-33</td>
</tr>
<tr>
<td>Displaying Proximity Probe Transfer Statistics</td>
<td>11-33</td>
</tr>
<tr>
<td>Displaying Proximity Status</td>
<td>11-35</td>
</tr>
<tr>
<td>Displaying Proximity Group Configuration</td>
<td>11-35</td>
</tr>
<tr>
<td>Displaying Proximity Database Status</td>
<td>11-36</td>
</tr>
<tr>
<td>Monitoring DNS Sticky Statistics on a GSS</td>
<td>11-37</td>
</tr>
<tr>
<td>Displaying DNS Rule Sticky Statistics</td>
<td>11-37</td>
</tr>
<tr>
<td>Displaying Sticky Statistics</td>
<td>11-38</td>
</tr>
<tr>
<td>Displaying Global Sticky Statistics</td>
<td>11-38</td>
</tr>
<tr>
<td>Displaying Global Sticky Mesh Statistics</td>
<td>11-40</td>
</tr>
<tr>
<td>Displaying Sticky Group Statistics</td>
<td>11-44</td>
</tr>
<tr>
<td>Displaying the Sticky Status</td>
<td>11-45</td>
</tr>
<tr>
<td>Displaying the Sticky Database Status</td>
<td>11-46</td>
</tr>
<tr>
<td>Displaying the Global Sticky Operating Status</td>
<td>11-47</td>
</tr>
<tr>
<td>Displaying the Global Sticky Mesh Operating Status</td>
<td>11-51</td>
</tr>
<tr>
<td>Displaying Sticky Group Configuration</td>
<td>11-56</td>
</tr>
<tr>
<td>Clearing GSS Global Server Load-Balancing Statistics</td>
<td>11-57</td>
</tr>
<tr>
<td>Monitoring Global Load-Balancing Statistics from the Primary GSSM GUI</td>
<td>11-58</td>
</tr>
<tr>
<td>Monitoring Answer Status and Statistics</td>
<td>11-58</td>
</tr>
<tr>
<td>Monitoring Answer Hit Counts</td>
<td>11-58</td>
</tr>
<tr>
<td>Monitoring Answer Keepalive Statistics</td>
<td>11-59</td>
</tr>
<tr>
<td>Monitoring Answer Status</td>
<td>11-60</td>
</tr>
<tr>
<td>Monitoring DNS Rule Statistics</td>
<td>11-61</td>
</tr>
<tr>
<td>Monitoring Domain Hit Counts</td>
<td>11-61</td>
</tr>
<tr>
<td>Monitoring Global Statistics</td>
<td>11-62</td>
</tr>
<tr>
<td>Monitoring Source Address Statistics</td>
<td>11-63</td>
</tr>
<tr>
<td>Monitoring DDoS Statistics</td>
<td>11-63</td>
</tr>
<tr>
<td>Monitoring Traffic Management Statistics</td>
<td>11-65</td>
</tr>
<tr>
<td>Monitoring Proximity Rule Hit Count Statistics</td>
<td>11-65</td>
</tr>
<tr>
<td>Monitoring Proximity Database Statistics</td>
<td>11-66</td>
</tr>
<tr>
<td>Monitoring Proximity Lookup Statistics</td>
<td>11-66</td>
</tr>
<tr>
<td>Monitoring Proximity Probe Management Statistics</td>
<td>11-67</td>
</tr>
<tr>
<td>Monitoring Sticky Rule Hit Statistics</td>
<td>11-67</td>
</tr>
<tr>
<td>Monitoring Sticky Database Statistics</td>
<td>11-68</td>
</tr>
<tr>
<td>Monitoring Global Sticky Mesh Statistics</td>
<td>11-68</td>
</tr>
</tbody>
</table>
Primary GSSM Global Server Load-Balancing Error Messages  A-1
Answer Error Messages       A-2
Answer Group Error Messages  A-3
Domain List Error Messages   A-5
DNS Rule Error Messages     A-7
KeepAlive Error Messages    A-11
Location Error Messages     A-13
Network Error Messages      A-13
Owner Error Messages        A-13
Proximity Error Messages    A-14
Region Error Messages       A-17
Source Address List Error Messages A-17
Sticky Error Messages      A-18
User Account Error Messages A-19
User Views Error Messages   A-19

Sticky and Proximity XML Schema Files  B-1
Sticky XML Schema File Contents B-2
Proximity XML Schema File Contents B-3

Glossary

Index
Preface

This guide includes information on configuring the Cisco Global Site Selector platform (GSS) from the primary GSSM GUI to perform global server load balancing. Certain global server load-balancing tasks require that you use the GUI, other tasks require that you use the CLI. In most cases, you have the option of using either the GUI or the CLI at the primary GSSM. Tasks that require you to use the CLI (configuring sticky groups, for example), are also described in this document.

This preface describes the following topics:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation and Submitting a Service Request

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:

<table>
<thead>
<tr>
<th>Chapter/Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introducing the Global Site Selector”</td>
<td>Describes the basic concepts underlying the GSS product as well as important GSS-related terms.</td>
</tr>
<tr>
<td>Chapter 2, “Configuring Resources”</td>
<td>Instructions on organizing resources on your GSS network as locations, regions, and owners.</td>
</tr>
<tr>
<td>Chapter 3, “Configuring Source Address Lists”</td>
<td>Describes the creation and modification of source address lists.</td>
</tr>
</tbody>
</table>
### Related Documentation

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

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Site Selector Hardware Installation Guide</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Regulatory Compliance and Safety Information for the Cisco Global Site Selector</strong></td>
<td>Provides regulatory compliance and safety information for the GSS platform.</td>
</tr>
<tr>
<td><strong>Release Note for the Cisco Global Site Selector</strong></td>
<td>Provides information on operating considerations, caveats, and new CLI commands for the GSS software.</td>
</tr>
<tr>
<td><strong>Cisco Global Site Selector Getting Started Guide</strong></td>
<td>Provides information on getting your GSS setup, configured, and ready to perform global server load balancing.</td>
</tr>
</tbody>
</table>
Symbols and Conventions

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

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Font</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Variables for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Screen examples use the following conventions:

<table>
<thead>
<tr>
<th>Font</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>screen</strong></td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>boldface screen</strong></td>
<td>Information you must enter is in <strong>boldface screen</strong> font.</td>
</tr>
<tr>
<td><em>italic screen</em></td>
<td>Variables for which you supply values are in <em>italic screen</em> font.</td>
</tr>
<tr>
<td>This pointer highlights an important line of text in an example.</td>
<td></td>
</tr>
<tr>
<td>^</td>
<td>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.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>
Graphical user interface elements use the following conventions:

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

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

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

1. A numbered list indicates that the order of the list items is important.
   a. An alphabetical list indicates that the order of the secondary list items is important.
   • A bulleted list indicates that the order of the list topics is unimportant.
      – An indented list indicates that the order of the list subtopics is unimportant.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
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 device.

This chapter contains the following major sections:

- GSS Overview
- DNS Routing
- Globally Load Balancing with the GSS
- GSS Architecture
- DDoS Detection and Mitigation
- GSS Network Deployment
- GSS Network Management
- Understanding the Primary GSSM GUI
- Global Server Load-Balancing Summary
- Where to Go Next
GSS Overview

Server load-balancing devices, such as the Cisco Content Services Switch (CSS), Cisco Content Switching Module (CSM), and Cisco Application Control Engine (ACE) 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, Cisco ACE, 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.

Note

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

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 FTP, and web surfing. DNS uses easy-to-remember alphanumeric host names 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 host names 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.
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, they are sent across the network in 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 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:

```
 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, 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 and higher, the default behavior is to reply to queries with negative responses; 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 v3.0 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 “Configuring an Authority Domain for 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.

The process outlined in 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

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 either:
   - Referring the D-proxy to the specific name server supporting 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 (192.168.1.1) to the client browser. The browser uses this IP address and initiates a connection to the www.cisco.com website.

**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 Application Control Engine (ACE) 4700 series appliance, ACE10-6500-K9 module, and ACE20-MOD-K9 module
- 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 8000 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 helps to ensure 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.

6. 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

1. Mobile
2. Fixed Wireless
3. Cable
4. DSL
5. Dedicated ATM/Frame Relay
6. ISDN/Dial

Client Name Servers (D-Proxy)
DNS Name Server
GSS 1
GSS 2
IP Global Forwarding Plane
DNS Global Control Plane
Data Center 1
Data Center 2
Data Center 3

--- Cisco GSS’s Response
--- Cisco GSS Tracking
--- Clients DNS Requests
--- Global Resources
--- Layer 3 Communications

Clients Requesting Web sites

Clients Requesting Web sites
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 and 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:

- GUI (graphical user interface) functions
- CLI commands, as described in the *Cisco Global Site Selector CLI-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.
**Chapter 1      Introducing the Global Site Selector**

**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.

---

**Note**

All mesh communications in the GSS network occurs over the IPv4 address. If you do not specify an IPv4 address the GSS services will not start.

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*.

IPv6 support has been extended to most functionalities. However by default, IPv6 is disabled on an interface. You can enable IPv6 support is enabled by configuring the IPv6 address on the interface. To enable the GSS functionality and to bring up the GSS communication, you need to configure IPv4 address on the interface. For more information, see *Cisco Global Site Selector CLI Configuration 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, region-sticky, and GeoDB 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.
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.

In addition to specific IP addresses, source addresses can also be set up to represent address blocks using variable-prefix-length classless interdomain routing (CIDR) block masking. The following examples illustrate acceptable GSS source IPv4 and IPv6 addresses:

IPv4

192.168.1.110
192.168.1.110/32
192.168.1.0/24
192.168.0.0/16

IPv6

2001:DB8::1
2001:DB8:0:ABCD::1
2001:DB8:2::1

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 GUI 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 domains cannot exceed 128 characters in length. The GSS supports domain names that use wildcards. The GSS also supports POSIX 1003.2-extended regular expressions when matching wildcards.

The following examples illustrate 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 4000 hosted domains and 4000 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 ACE, 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.
- 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 GUI 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 ACE is routed to the best resource based on load and availability, as determined by the ACE. 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 about 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 because of 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

When a client D-proxy sends a query to a GSS configured to use external name servers, the following sequence of actions occur:

1. The GSS performs a global server load balancing (GSLB) lookup on the query to see if the answer is contained within its database. The GSS performs one of the following actions depending on the answer type and the answer operating state:
   - If the answer type is VIP and the answer is online, the GSS sends the answer to the client D-proxy.
If the answer type is VIP and the answer is offline, the GSS retrieves and sends a fallback answer to the client D-proxy.

If the last clause answer type is VIP and the answer is offline, the GSS sends a SERVFAIL response to the client D-proxy.

If the answer type is NS, the GSS forwards the query to the name server called for in the NS Forwarding definition. The name server responds to the D-proxy through the GSS (the GSS acts as a proxy).

2. If the GSS performs a GSLB lookup and cannot find an answer to the query, the GSS sends a negative response (NXDOMAIN) to the client D-proxy.

### 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 explain the various keepalive types supported by the GSS:

- Multiport Keepalives
- ICMP
- TCP
- HTTP HEAD
- HTTPS 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, a Cisco ACE, 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.
**Chapter 1      Introducing the Global Site Selector**

**GSS Architecture**

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

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 web servers, Local Directors, 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 up to 1500 TCP keepalives when using the standard detection method and up to 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 ACE, Cisco IOS-compliant SLB, or Cisco Local Director. 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.

HTTPS HEAD

The HTTPS HEAD keepalive probe type to its existing list of probe types used to determine a host device’s serviceability status. The list of probe types that GSS supports now consists of ICMP, TCP, HTTP HEAD, HTTPS-HEAD, KAL-AP, Scripted KAL, CRA, and Name Server. The GSS uses the new HTTPS HEAD keepalive to monitor the status of the HTTPS application running on a secure Web server. Monitoring is performed using default port 443.

To access this feature from the GUI, choose one of the following:

- DNS Rules > Answers > Create > VIP
- DNS Rules > Shared Keepalives > Create
- Resources > Keepalive Properties

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 more 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 named 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.

**Note**
For ICMP standard keepalive, retry count is 3 and response timeout is 10 seconds. And, for NS keepalive, retry count is 0 and response timeout is 10 seconds.

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

\[
(# \text{ Ack'd Packets} \times (\text{Response TO} + (\text{Retry TO} \times \# \text{ of Retries}))) + \text{Timed Wait}
\]

where:
- \# \text{ 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**

<table>
<thead>
<tr>
<th></th>
<th># Ack’d Packets (Fixed Value)</th>
<th>Response TO (Fixed Value)</th>
<th>Retry TO (Fixed Value)</th>
<th># of Retries (User Selectable)</th>
<th>Timed Wait (Fixed Value)</th>
<th>Transmission Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>KAL-AP</td>
<td>1</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>0</td>
<td>4 seconds</td>
</tr>
<tr>
<td>ICMP</td>
<td>1</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>0</td>
<td>4 seconds</td>
</tr>
<tr>
<td>TCP (RST)</td>
<td>1</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>0</td>
<td>4 seconds</td>
</tr>
<tr>
<td>TCP (FIN)</td>
<td>2</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>2 seconds</td>
<td>10 seconds</td>
</tr>
</tbody>
</table>
For a TCP (RST) connection, the default transmission interval for a TCP keepalive is as follows:

\[(1 \times (2 + (2 \times 1))) + 0 = 4 \text{ seconds}\]

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:

\[(1 \times (2 + (2 \times 5))) + 0 = 12 \text{ seconds}\]

Figure 1-5 shows the effect on the keepalive transmission interval as you increase the number of retries value.

### Table 1-1 Keepalive Transmission Rates for a Single Keepalive Per Answer (continued)

<table>
<thead>
<tr>
<th>HTTP HEAD (RST)</th>
<th># Ack’d Packets (Fixed Value)</th>
<th>Response TO (Fixed Value)</th>
<th>Retry TO (Fixed Value)</th>
<th># of Retries (User Selectable)</th>
<th>Timed Wait (Fixed Value)</th>
<th>Transmission Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>0</td>
<td>8 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP HEAD (FIN)</th>
<th># Ack’d Packets (Fixed Value)</th>
<th>Response TO (Fixed Value)</th>
<th>Retry TO (Fixed Value)</th>
<th># of Retries (User Selectable)</th>
<th>Timed Wait (Fixed Value)</th>
<th>Transmission Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>2 seconds</td>
<td>2 seconds</td>
<td>1</td>
<td>2 seconds</td>
<td>14 seconds</td>
</tr>
</tbody>
</table>
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 number of successful probes parameter 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 contains the following topics:

- Ordered List Method
- Round-Robin Method
- Weighted Round-Robin Method
- Least-Loaded Method
- Hashed Method
- DNS Race (Boomerang) Method
- Balance Method Options for Answer Groups
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 used only if preceding VIPs or name servers on the list are unavailable. The GSS supports gaps in numbering in an ordered list.

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 or Scripted 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.
Chapter 1      Introducing the Global Site Selector

See the “Balance Method Options for Answer Groups” section for information on 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

<table>
<thead>
<tr>
<th>Answer Type</th>
<th>Balance Methods Used</th>
<th>Answer Group Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>Hashed</td>
<td>Order</td>
</tr>
<tr>
<td></td>
<td>Least-loaded</td>
<td>LT (Load Threshold)</td>
</tr>
<tr>
<td></td>
<td>Ordered list</td>
<td>Weight</td>
</tr>
<tr>
<td></td>
<td>Round-robin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weighted round-robin</td>
<td></td>
</tr>
<tr>
<td>Name server</td>
<td>Hashed</td>
<td>Order</td>
</tr>
<tr>
<td></td>
<td>Ordered list</td>
<td>Weight</td>
</tr>
<tr>
<td></td>
<td>Round-robin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weighted round-robin</td>
<td></td>
</tr>
<tr>
<td>CRA</td>
<td>Boomerang (DNS race)</td>
<td>None</td>
</tr>
</tbody>
</table>

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 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 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 undisturbed 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 9, 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 proximity probing agent, a Cisco IOS-based router or a GSS configured as a DRP agent, 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 10, Configuring Network Proximity, for information about configuring proximity for GSS devices in your network.

**Geo-Location-Based GSLB Feature**

GSS software Version 4.1(0) supports the GeoIP database (GeoDB) proximity computation mechanism in GSS. From the latitudinal and longitudinal information in the GeoDB, GSS decides the proximity, based on the geographical distance from the client D-proxy instead of the round-trip time (RTT) value.

During the proximity calculation, the GSS uses these distances instead of RTT values to determine the IP address of the resource nearest to the D-proxy.

To enhance the various GSS features with GeoIP-awareness, you can add support for the GeoDB in locations. The process of updating the GeoDB does not impact GSS operations. All user-defined database entries are preserved during a database upgrade.

To enable the GeoDB feature, a valid license should be installed and the GeoIP database should be imported into GSS. After importing, if static entries are present, then the distance gets computed based on latitude and longitude mentioned for the static entries.

GSS software Version 4.1(0) supports the capability to answer DNS requests with most proximate answers to the D-proxy.

The GeoDB sticky module supports the following IPv6 functionalities in software Version 4.1.0:

1. Global prefix length can be configured to match IPv6 D-Proxy addresses into the same sticky database (SDB) entry.
2. The Sticky Groups can be configured for IPv6 address. The IPv6 D-Proxy addresses and the answers returned for AAAA queries can be stored to track hit count for AAAA query answers.
3. All sticky database operations like SDB lookup and SDB entry delete operations should be enhanced for IPv6 D-Proxy and IPv6 answers.
4. The IPv6 sticky database can be synced across the GSS mesh when the global sticky is used.

If you want to enable the GeoDB license package on a particular GSS, you must purchase a GeoDB license from Cisco Systems to receive a Product Authorization Key (PAK) number. For more information on obtaining and installing a GeoDB license, see the Global Site Selector Administration Guide.
DDoS Detection and Mitigation

Distributed Denial of Service (DDoS) attacks are designed to deny legitimate users access to a specific computer or network resource by flooding the target with traffic from a single host or from multiple hosts. These attacks may send several thousand spoofed DNS requests to a target device. The target then treats these requests as valid and processes the malicious requests.

Because the target is busy replying to the attack, it drops valid DNS requests from legitimate D-proxies. When the number of requests is in the thousands, the attack 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 types of attacks:

- 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

Note

You enable DDoS prevention and configure filters, rate limits, and anti-spoofing using the CLI. See the Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide for specific procedures.
**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](image)

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

- DNS packets are dropped if they come from a source port other than 53.
- DNS packets are dropped if they have a destination port of 53.
- DNS packets are dropped with a source port neither equal to 53 nor greater than 1024.

By default, mitigation rules are enabled.

**Rate Limits**

The GSS enforces a limit on the number of DNS packets per minute for each individual D-proxy and an overall global rate limit. 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 `scaling-factor global` CLI commands in ddos configuration mode.

The GSS also enforces a rate limit (unknown rate-limit) that limits the number of anti-spoofing tests to be performed by the GSS in a minute. Once this limit is reached, the GSS drops DNS packets from new sources during that minute. By default, the GSS performs spoof tests for 1000 new D-proxies per minute. You can change this limit by configuring the unknown rate limit.

The GSS enforces rate limits for DNS traffic only; it does not enforce limits for all traffic. You can configure the rate limit for DNS packets from a particular D-proxy only by providing the IP address.
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. It is based on forcing the client to resend its query using TCP. The D-proxy sends a UDP request, and the GSS responds with TC or truncated bit. If the D-proxy replies using TCP and the TCP handshake is successful, then the GSS sends the TCP reply and considers the D-proxy to be valid for one hour. DDoS allows only traffic from such D-proxies to pass to the selector.

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.

Nonspoofed D-proxies stay trusted for one hour. This nonspoofed timeout is not configurable.

If an anti-spoofing check fails (there is no response to the TCP connection), the D-proxy is blacklisted for one minute. This spoofed timeout is not configurable.

You may disable anti-spoofing for a particular D-proxy if that D-proxy does not support the option to respond using TCP. You can manually configure a D-proxy as either trusted or spoofed. If you configure a D-proxy as trusted, the GSS does not perform the anti-spoofing test for that IP address. If you configure a D-proxy as spoofed, the GSS drops all requests from that IP address.

See Chapter 11, Monitoring GSS Global Server Load-Balancing Operation, for instructions on how to monitor DDoS statistics.
GSS Network Deployment

A GSS deployment may contain a maximum of 16 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 GSS 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 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 on modifying your network’s 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 you position your GSS behind a firewall or enable packet filtering on the GSS itself, be sure to 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 ACE, 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.

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 through the creation of DNS rules and monitoring of keepalives
- Monitor GSS network resources
- Monitor request routing and GSS statistics

For more information about the GUI, see the “Understanding the Primary GSSM GUI” section.
Chapter 1  Introducing the Global Site Selector

Understanding the Primary GSSM GUI

The primary GSSM graphical user interface is a web-based tool that you access using any standard web browser such as Microsoft Internet Explorer Version 5.0 and later releases and Mozilla Firefox Version 3.6.3 or later releases. Basic authentication is used to restrict GUI access. All GUI traffic is encrypted using secure HTTP (HTTPS).

The primary GSSM GUI serves as a centralized management point for your entire GSS network. Using the primary GSSM GUI, you can add GSS devices to your network and build DNS rules that match groups of source addresses to hosted domains using one of a number of possible load-balancing methods. In addition, using the GSSM monitoring feature allows you to obtain real-time statistics on the performance of your GSS network or of individual devices on that network.

After you log on to the primary GSSM GUI, the Welcome window (see Figure 1-7) appears. The current login account information appears in the User ID (upper right) area of the Welcome window.

Figure 1-7  Primary GSSM Welcome Window

This section describes the organization and structure of the primary GSSM GUI and contains the following topics:

- GUI Organization
- List Pages
- Details Pages
- Navigation
- Primary GSSM GUI Icons and Symbols
- Primary GSSM GUI Online Help

Review this information before using the primary GSSM GUI to define global load balancing for your GSS network.
GUI Organization

The primary GSSM GUI is organized into five main functional areas. Each area is divided by tabs, that you click to navigate to a particular section of the primary GSSM. These functional areas are as follows:

- **DNS Rules Tab**—Pages for creating and modifying DNS rules, including the creation of source address lists, (hosted) domain lists, answers, answer groups, and shared keepalives.
- **Resources Tab**—Pages for creating and modifying GSS network resources such as GSSs, locations, regions, and owners. You can also modify global keepalive properties from the Resources tab.
- **Monitoring Tab**—Pages for monitoring the performance of content routing on your GSS network, such as displays of hit counts organized by source address, domain, answer method, or DNS rule.
- **Tools Tab**—Pages for performing the administrative functions for the GSS network, such as creating login accounts, managing account passwords, and viewing system logs.
- **Traffic Mgmt Tab**—Pages for configuring the advanced global server load-balancing functions, DNS sticky, and network proximity

You access specific pages within each functional area by choosing from a series of navigation links in the upper left corner of the GUI. The navigation links vary according to the selected tab. Navigation links are available on all GUI pages.

Once you select a page, information is further organized into two areas: list pages and details pages.

**List Pages**

List pages provide you with a feature-specific overview. For example, you click the Answers tab (located on the DNS Rules tab) to display the Answers list page. This list page shows all of the answers currently configured on the listed GSS network.

List pages display all data in tabular format to provide you with a detailed view of the resources available on your GSS network. In addition, you can use list pages to add new resources (for example, DNS rules or answer groups) or modify existing resources.

List pages enable you to sort resources by any one of a number of properties listed on the page. You can quickly locate a particular resource by using an identifying characteristic such as a name, owner, or type. You can sort information in ascending or descending order by any column. To sort the information in a list page, click the column header for the column that contains the information you want to sort.

The GSS software temporarily retains information that you modify for a list page, allowing you to navigate to any of the details pages associated with the active list page while retaining the list page settings. The sort field, sort order, and rows per page are temporarily stored in memory for the active list page. Once you navigate to another list page, the GSS software discards the modifications for the previous list page.

**Details Pages**

Details pages provide specific configuration information for a specific GSS function, enabling you to define or to modify those properties. You access a details page from a list page.

For example, click the Answers navigation link to display the Answers list page. Next to each answer is an icon that shows a pad and pencil, called the Modify icon. Click the Modify icon to display the details page for that answer. From the Modifying Answer details page, modify the properties of an answer or delete the answer.
Navigation

The primary GSSM GUI is viewed as a series of web pages using a standard browser. However, navigating between primary GSSM GUI pages is not the same as moving around different websites or even within a single site. Instead, you navigate from one content area of the GUI using the tabs for each of the major functional areas: DNS Rules, Resources, Monitoring, Tools, and Traffic Mgmt. Online Help is located as a navigation link at the top of each page.

Once you are located within a major content area, you can then access a particular feature or move between features using the navigation links. Choosing a feature from the navigation links immediately transfers you to that page in the graphical user interface. To move back from a details page to the corresponding list page, click another navigation link, or click either the Submit or Cancel buttons from the details page.

For example, to return to the Global Site Selectors list page after viewing the details for one of your GSS devices, click a different navigation link (or click the Cancel button). If you made configuration changes to a GSS that you wish to retain, click the Submit button. Any of these actions returns you to the Global Site Selectors list page.

Note: Do not use your web browser Back or Forward buttons to move between pages in the primary GSSM GUI. Clicking Back cancels any unsaved changes in the primary GSSM.

Primary GSSM GUI Icons and Symbols

Table 1-3 lists and explains some common icons and graphical symbols in the primary GSSM GUI. These icons are referenced throughout this publication to explain how to use the features of the primary GSSM GUI.

Table 1-3  GSSM GUI Icons and Symbols

<table>
<thead>
<tr>
<th>Icon or Symbol</th>
<th>Purpose</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Modify icon. Opens the associated item for editing in a details page, displaying configuration settings on the details page.</td>
<td>List pages</td>
</tr>
<tr>
<td></td>
<td>Sort icon. Indicates that the items listed in a list table are sorted in descending order according to the property listed in this column.</td>
<td>List pages</td>
</tr>
<tr>
<td></td>
<td>Create icon/Open DNS Rules Builder icon. Opens the associated details page to accept user input for configuration.</td>
<td>List pages</td>
</tr>
<tr>
<td></td>
<td>Print icon. When you view GSS resources or monitor GSS network activity, Print allows you to print data displayed in the page using your local or network printer.</td>
<td>List pages and Detail pages</td>
</tr>
<tr>
<td></td>
<td>Export to CSV icon. When you view GSS resources or monitor GSS network activity, Export allows you to save data displayed in the window to a comma-delimited flat file for use in other applications.</td>
<td>List pages</td>
</tr>
</tbody>
</table>
### Table 1-3 GSSM GUI Icons and Symbols (continued)

<table>
<thead>
<tr>
<th>Icon or Symbol</th>
<th>Purpose</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Refresh icon" /></td>
<td>Refresh icon. When you view GSS resources or monitor GSS network activity, Refresh forces the GUI page to update its content.</td>
<td>List pages</td>
</tr>
<tr>
<td><img src="image" alt="Run Wizard icon" /></td>
<td>Run Wizard icon. Opens the associated DNS rule for editing using the DNS Rules Wizard.</td>
<td>DNS Rules list page</td>
</tr>
<tr>
<td><img src="image" alt="Filter DNS Rule List icon" /></td>
<td>Filter DNS Rule List icon. Provides filters that can be applied to your DNS rules, allowing you to view only those rules that have the properties in which you are interested.</td>
<td>DNS Rules list page</td>
</tr>
<tr>
<td><img src="image" alt="Show All DNS Rules icon" /></td>
<td>Show All DNS Rules icon. Removes all filters, displaying a complete list of DNS rules for your GSS.</td>
<td>DNS Rules list page</td>
</tr>
<tr>
<td><img src="image" alt="Asterisk" /></td>
<td>Asterisk. Required field. Indicates that a value is required in the adjacent field before the item can be successfully saved.</td>
<td>Details pages</td>
</tr>
<tr>
<td><img src="image" alt="Submit icon" /></td>
<td>Submit icon. Saves the configuration information. When editing specific GSS system or device configuration information, Submit returns you to the associated list screen.</td>
<td>Detail pages</td>
</tr>
<tr>
<td><img src="image" alt="Cancel icon" /></td>
<td>Cancel icon. Cancels any configuration changes that were entered. When editing specific GSS system and device configuration information, Cancel returns you to the associated list screen.</td>
<td>Detail pages</td>
</tr>
<tr>
<td><img src="image" alt="Delete icon" /></td>
<td>Delete icon. When you view configuration information for GSS resources, Delete allows you to delete the resource from the GSS network.</td>
<td>Detail pages</td>
</tr>
<tr>
<td><img src="image" alt="Note" /></td>
<td><strong>Note</strong> Deletions of any kind cannot be undone in the primary GSSM GUI. If you might want to use the deleted data at a later point in time, we recommend performing a database backup of your GSSM. See the Cisco Global Site Selector Administration Guide for details.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Next icon" /></td>
<td>Next icon. Moves forward to the next page in the DNS Rules Wizard. You can also use the links under the Wizard Contents table of contents to move between steps in the wizard.</td>
<td>DNS Rules wizard</td>
</tr>
<tr>
<td><img src="image" alt="&lt; Back" /></td>
<td>Back icon. Moves back to the previous page in the DNS Rules Wizard. You can also use the links under the Wizard Contents table of contents to move between steps in the wizard.</td>
<td>DNS Rules wizard</td>
</tr>
</tbody>
</table>
Primary GSSM GUI Online Help

The Help navigation link in the upper right corner of each primary GSSM GUI page launches the Online Help system, which contains information on using that page as well as the features of the primary GSSM GUI. The Online Help topic associated with the form displays in a separate child browser window.

Each page in the primary GSSM GUI has a context-sensitive online Help file associated with it. These Help files (in HTML format) contain detailed information related to the form that you are using. Online Help also includes a series of quick-start procedures to assist you in navigating through the specific forms in the user interface and performing specific configuration procedures (for example, using the DNS Rules wizard to create a DNS rule).
The GSS Online Help system contains several navigational aids to assist you in finding the information that you need quickly and easily. The navigation frame is contained in the left frame of each Help topic. The navigation frame contains the following three tabs:

- **Contents**—Displays all the topics in the GSSM Online Help system in a tiered format. Help topics are grouped into logical books by function. Books of Help topics may contain sub-books with additional topics. You can expand or collapse the contents to suit your needs. Note that the contents also automatically synchronizes with the Help topic that you are currently viewing.

- **Index**—Displays a list of terms that allows you to look up topics based on keywords similar to the index at the back of a book. If only one topic is associated with the Index entry, that topic displays immediately when you double-click the entry. If more than one topic is associated with an Index entry, the Help system displays a Topics Found dialog box that allows you to select the topic that you want to display from a list of topics.

- **Search**—Provides a full-text search tool that allows you to display a list of Help topics related to words that you enter in the text box. You can then select a topic and click **Display** to view that topic.

### 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 about getting your GSSM (primary and standby) and GSS devices set up, configured, and ready to perform global server load balancing.

You use the centralized GUI on the primary GSSM to configure global server load balancing for your GSS network. Using this interface, 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.

Because you create DNS rules that route incoming DNS requests to the most available data centers and resources on your network, you must configure the elements that constitute your DNS rules before creating the rules themselves.

To configure your GSS devices and resources from the primary GSSM for global server load balancing, perform the following sequence of 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. These GSS network resources are regularly polled to monitor the online status of one or more GSS resources linked to the keepalive. Shared keepalives are required for any answer that uses the KAL-AP keepalive type. See Chapter 5, Configuring Keepalives, for details.

5. **Create one or more answers and answer groups**—Answers are resources that match requests to domains. Answer groups are collections of resources that balance requests for content. See Chapter 6, Configuring Answers and Answer Groups, for details.
6. Build the DNS rules that will control global server load balancing on your GSS network. See Chapter 7, Building and Modifying DNS Rules, for details.

7. If you plan to use DNS sticky for your global server load balancing, 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 9, 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 10, Configuring Network Proximity, for details.

Where to Go Next

Chapter 2, Configuring Resources describes how to organize resources on your GSS network as locations, regions, and owners.
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
- Creating and Modifying Locations and Regions
- Creating and Modifying Owners
- Grouping GSS Resources by Location, Region, and Owner
- Managing Global Manual Reactivation of Answers and Clauses
- Where to Go Next
Organizing Your GSS Network

The primary GSSM provides you the following ways 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 are not required to correspond to actual geographical sites. They are simply organizing concepts that allow you to group GSS resources and exist in a one (region) to many (locations) relationship.

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.

Creating and Modifying Locations and Regions

Use the following procedures to set up regions and locations on your GSS network.

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

Note
Release 4.1.0 supports creating additional regions and adding states to a specific region.

This section contains the following topics:

- Creating Regions
- Modifying Regions
- Add or Modify Regions and States
- Creating Locations
- Modifying Locations
- Deleting Locations and Regions

Creating Regions

To create a region, perform the following steps:
1. From the primary GSSM GUI, click the Resources tab.
2. Click the Regions navigation link. The Regions list page appears.
3. Click the **Create Regions** icon. The Creating New Region details page appears.

4. In the Name field, enter the name for your new region.

5. In the Comments field, enter descriptive information or important notes regarding the new region.

6. Click **Submit** to save changes to your new region and return to the Region list page. Your new region appears in the list and can be used to help you organize other GSS resources.

---

**Note**
The recommended maximum number of regions you can create is 20.

---

### Modifying Regions

To modify a GSS region, perform the following steps:

1. From the primary GSSM GUI, click the **Resources** tab.

2. Click the **Regions** navigation link. The Regions list page appears.

3. From the Regions list, click the **Modify Region** icon located to the left of the list that you want to modify. The Modifying Region details page appears.

4. In the Name field, change the name of the region, if desired.

5. In the Comments field, enter or modify the descriptive information or notes regarding the region.

6. Click **Submit** to save the changes to your region and return to the Regions list page.

---

### Add or Modify Regions and States

To add or modify a state in the regions from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Resources** tab.

2. Click the **Regions** navigation link. The Regions details page appears listing all of the configured regions.

3. Click the **Create Regions** (+) icon. The Creating New Region - General Configuration details page appears.

4. In the Name field, enter the name for your new Region.

5. In the Comments field, enter descriptive information or important notes regarding the Region.

6. To add a state in a selected region, click **Add States** from the navigation bar on the left. The modifying region details page appears.

---

**Note**
The primary GSS GUI supports specific countries and regions. Before you add or modify the regions or states, you have to import the GeoDB database file. To import the GeoDB database file, use the following command:

```
geodb database import tar-file-name cisco_geodb_2011-07-12_v001.tar.gz
md5sum-file-name cisco_geodb_2011-07-12_v001.tar.gz.md5
```

Download the GeoDB database file from the following URL: [http://geolite.maxmind.com/download/sec/](http://geolite.maxmind.com/download/sec/). To enable the database file, username, and password, refer to the e-delivery letter of your GeoIP license. For further assistance, contact your Cisco account representative.
Creating and Modifying Locations and Regions

Chapter 2 Configuring Resources

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.

Creating Locations

To create a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Create Location icon. The Creating New Location details page appears.
4. In the Name field, enter the name for your new location.
5. Click the Region drop-down list and choose a region with which the location will be associated. There should be a logical connection between the region and location.

6. If performing network proximity, click the Zone drop-down list and associate a zone with the location. There should be a logical connection between the zone and the location.

7. In the Comments field, enter descriptive information or important notes regarding the new region or location.

8. Click Submit to save your new location and return to the Locations list page. Your new location appears in the list and can be used to help you organize other GSS resources.

Modifying Locations

To modify a GSS location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.

2. Click the Locations navigation link. The Locations list page appears.

3. From the Locations list, click the Modify Location icon located to the left of the list that you want to modify. The Modifying Location details page appears.

4. In the Name field, change the name of the location, if desired.

5. If you wish to move the location to a new region, click the Region drop-down list and select a new region with which the location will be associated.

6. If performing network proximity, click the Zone drop-down list and associate a zone with the location. There should be a logical connection between the zone and the location.

7. In the Comments field, enter or modify the descriptive information or notes regarding the location.

8. Click Submit to save the changes to your location and return to the Locations list page.

Deleting Locations and Regions

Before deleting a region or location, ensure that you know about the dependencies associated with a resource. For example, regions that have locations associated with them cannot be deleted. In addition, 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.

To delete regions and locations, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.

2. Click either the Locations or Regions navigation link, depending on what type of resource you want to delete. The list page appears.

3. Click the Modify icon for the location or region that you want to delete. The details page appears, displaying configuration information for that resource.

4. Click the Delete icon in the upper-right corner of the page. The GSS software prompts you to confirm your decision to delete the Region or Location.
Creating and Modifying Owners

Creating Owners

To create an owner, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Owners navigation link. The Owners list page appears displaying a list of all configured owners on your GSS network and providing an overview of the resources assigned to each owner.
3. Click the Create Owner icon. The Creating New Owner details page appears.
4. In the Name field, enter the contact name for your new owner.
5. In the Comments field, enter other descriptive or contact information for the new owner.
6. Click Submit to save the new owner and return to the Owners list page. Your new owner is listed and can now be used to help you organize other GSS resources.

Modifying Owners

To modify an owner, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Owners navigation link. The Owners list page appears.
3. From the Owners list, click the Modify Owner icon located to the left of the list that you want to modify. The Modifying Owner details page appears.
4. In the Name field, enter a new name for your new owner, if desired.
5. In the Comments field, enter or modify the descriptive information or notes regarding the owner.
6. Click Submit to save the changes to the owner and return to the Owners list page.

Deleting Owners

Before you attempt to delete an owner, be sure that you know the dependencies of that resource. For example, answer groups, DNS rules, and domain lists associated with an owner will, if that owner is deleted, 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, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Owners navigation link. The Owners list page appears.
3. From the Owners list, click the Modify Owner icon located to the left of the list that you want to delete. The Modifying Owner details page appears.
4. Click the Delete icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the owner.
5. Click OK to confirm your decision. You return to the Owners list page.

Grouping GSS Resources by Location, Region, and Owner

After you create your locations, regions, and owners, you can begin to use these tools to help organize your GSS resources. To associate a particular resource with a location, region, or owner, edit the properties of that resource and then choose the location, region, or owner from the drop-down list provided. Table 2-1 indicates which GSS resources can be grouped by locations, regions, and owners.

<table>
<thead>
<tr>
<th>GSS Network Resource</th>
<th>Grouped By</th>
<th>Grouped Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSS</td>
<td>Location</td>
<td>Global Site Selector details page</td>
</tr>
<tr>
<td>Locations</td>
<td>Region</td>
<td>Locations details page</td>
</tr>
<tr>
<td>Region</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Owner</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>DNS rules</td>
<td>Owner</td>
<td>DNS Rule Builder</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td>DNS Rule Wizard</td>
</tr>
<tr>
<td>Source address lists</td>
<td>Owner</td>
<td>Source Address Lists details page</td>
</tr>
<tr>
<td>Domain lists</td>
<td>Owner</td>
<td>Domain Lists details page</td>
</tr>
<tr>
<td>Answer group</td>
<td>Owner</td>
<td>Answer Group details page</td>
</tr>
<tr>
<td>Answer</td>
<td>Location</td>
<td>Answer details page</td>
</tr>
</tbody>
</table>
Managing Global Manual Reactivation of Answers and Clauses

Use the GSS manual reactivation function to manage when the GSS reverts to sending an answer that had gone offline but is now online and ready for service, or reverts to using a clause that was unavailable for use but is now available and ready for service.

The manual reactivation function works as follows for answers and clauses:

- **Answers**—When an answer goes offline (for example, Answer 1), the GSS sends the next available answer (Answer 2) associated with the clause. If the clause does not contain another answer to send, the GSS sends an answer from the next available clause. By default, the GSS reverts to sending Answer 1 when this answer returns to an online state. To manually control when the GSS reverts to sending an answer that returns to an online state after being offline, you enable the manual reactivation feature from the primary GSSM.

  When you enable manual reactivation for a specific answer and a GSS on the GSS mesh detects that its local copy of the answer is offline, that GSS alone suspends its copy of the answer. The GSS marks the answer as “operational suspend” and does not use it in its load-balancing algorithm. KALs do not monitor the suspended answer, which remains suspended until you reactivate all operationally suspended answers. Because the other GSSs on the GSS mesh maintain their own operational view of the answer, they continue to treat it as online as long as it remains in an online state locally.

- **Clauses**—A clause becomes unavailable for use by the GSS when all the answers in the answer group associated with it are either offline or overloaded. When at least one of the answers returns to an online state, the clause becomes available once again and the GSS, by default, begins using it. To manually control when the GSS reverts to using a clause that returns to an available state, you enable the manual reactivation function from the primary GSSM.

  When you enable manual reactivation for a specific clause and a GSS on the GSS mesh detects that its local copy of the clause is unavailable, that GSS alone suspends its copy of the clause. The GSS marks the clause as “operational suspend” and does not use it in its load-balancing algorithm. Because the other GSSs on the GSS mesh maintain their own operational view of the clause, they continue to treat it as online as long as it remains in an online state locally. The clause remains suspended until you reactivate all operationally suspended clauses.

To use the manual reactivation function for answers and clauses, you must configure the primary GSSM as follows:

- Enable manual reactivation in each answer that you want to manage (see the “Configuring and Modifying Answers” section on page 6-1).
- Enable manual reactivation in each clause that you associate with a rule and want to manage (see the “Building DNS Rules Using the DNS Rule Builder” section on page 7-10).
- Enable the global manual reactivation function as described in this section. The global manual reactivation function enables the GSS to operationally suspend all answers or clauses that you configure for manual reactivation. You can then manually reactivate all answers or clauses that are in the Operational Suspend state when required.

This section contains the following topics:

- **Enabling or Disabling the Global Manual Reactivation Function**
- **Activating All Operationally Suspended Answers or Clauses**
Enabling or Disabling the Global Manual Reactivation Function

To enable or disable the global manual activation function on the primary GSSM, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
3. Click the desired manual reactivation operating state:
   - **Disabled**—Disables the manual reactivation function.
   - **Enabled**—Enables the manual reactivation function.
4. Click Submit to save the manual reactivation change.

### Note
Disabling global manual reactivation causes the GSS to automatically reactivate all answers and clauses when they return to an online state, including any answers and clauses that you configure for manual reactivation.

### Activating All Operationally Suspended Answers or Clauses

You can manually reactivate all of the answers or clauses that the GSS operationally suspended.

#### Note
Manually reactivating all of the answers that the GSS operationally suspended restarts all of the keepalives for answers that have manual reactivation enabled, including those that are currently in an online state. This may cause the online manual reactivation answers to enter the initializing (INIT) state for a short period of less than 40 seconds before returning to an online state.

To manually reactivate all of the answers or clauses that are operationally suspended, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
3. Click the Activate MR-enabled answers/clauses drop-down list and choose one of the following options:
   - **Activate MR-enabled answers**—Reactivates all answers that are currently in an Operational Suspend state.
   - **Activate MR-enabled clauses**—Reactivates all clauses that are currently in an Operational Suspend state.
4. Click Submit to activate the chosen manual reactivation option.

Where to Go Next

Chapter 3, Configuring Source Address Lists, describes the creation of source address lists, which 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. You configure GSS request handling by creating source address lists, which are collections of IP addresses or address blocks 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.

In addition to adding individual addresses, the primary GSSM also allows you to enter IP address blocks conforming to the classless interdomain routing (CIDR) IP addressing scheme.

This chapter contains the following major sections:

- Creating Source Address Lists
- Modifying Source Address Lists
- Deleting Source Address Lists
- Where to Go Next
Creating Source Address Lists

The state codes and country codes sometimes disappear if you perform `geodb enable | disable` function after you import the GeoDB database file. This change occurs because the country and state codes, that are needed to create regions is stored as a GSLB configuration. It is recommended that you import the GeoDB database file again for the proper functionality. The executing `show geodb output` command displays the status of the GeoDB tables that are available in the cache memory, where as the codes reside in the gslb configuration.

Note

When you configure the GSS with an IP-based source address list and region-based source address list, the DNS lookup for an IP address-based source address list takes precedence over region-based source address list. The DNS lookup for the source address list that has been configured with `anywhere (0.0.0.0/0, ::/0)` takes the least priority.

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

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Source Address Lists navigation link. The Source Address Lists list page appears.
3. Click the Create Source Address List icon. The Creating New Source Address List details page appears.
4. In the General Configuration details page (General Configuration navigation link), perform the following:
   a. In the Name field, enter a name for the new Source Address List. Source Address List names cannot contain spaces.
   b. From the Owner drop-down list, select the GSS network resource with which the Source Address List is associated. The owner may be a hosting customer, an internal department such as human resources, or an IT staff resource.
   c. In the Comments text area, enter any comments for the new Source Address List.
5. Click the Add Address navigation link to access the Add Addresses section of the page. Add new addresses or address blocks to your list of source addresses.
6. In the Add Addresses section of the page, perform the following:
   a. Enter the IP addresses or Classless Inter-Domain Routing (CIDR) address blocks of the client DNS proxies. You use this interface to add new addresses or address blocks to your list of source addresses. If entering multiple addresses, separate each address with a semicolon. You can enter up to 30 addresses for each list. Enter either an IPv4 or IPv6 address. For example, 192.168.100.0/24; 10.89.0.0/16; 10.68.10.1 or 2001:DB8::1; 2001:DB8::/32.
   b. Click the Add button. The GSS software adds the addresses to the Source Address List.
7. Click the General Configuration navigation link to view the address block associated with the source address list. The addresses appear under the Current Members section of the details page.
8. Click the Submit button to save your changes and return to the Source Address Lists list page.
Modifying Source Address Lists

To modify an existing source address list, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Modify Source Address List icon located to the left of the Source Address List that you want to modify. The Modifying Source Address List details page appears.
3. In the General Configuration details page (General Configuration navigation link), use the fields provided to modify the name, comments, or owner for the source address list. Source address list names cannot contain spaces.
4. Click the Add Addresses navigation link to add more source addresses to the list. Use the field provided to enter the names of source address lists that you want to add. Click the Add button to append the new source address to the existing list.
5. Click the Remove Addresses navigation link to remove addresses from the Source Address List. The Remove Addresses section of the page appears. Click the check box accompanying each source address that you want to remove from the list, and then click the Remove Selected button to remove the selected source addresses from the list.
6. Review your updated source address list under the Current Members section of the details page.
7. To add regions from the source address list, click the Add Regions navigation link. Choose the region from the Add Regions drop-down list, and then click the Add button.
8. To remove regions from the source address list, click the Remove Regions navigation link. Click the check box accompanying each region you wish to remove from the list, then click the Remove Selected button to remove the selected regions from the list.
9. Click the Submit button to save your modified source address list and return to the Source Address List list page.

Deleting Source Address Lists

You cannot delete source address lists associated with an existing DNS rule. Before deleting a source address list, first verify that none of your DNS rules reference the source address list that you are to delete. If necessary, deselect 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 from your GSS network, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Source Address Lists navigation link. The Source Address Lists list page appears.
3. Click the Modify Source Address List icon located to the left of the Source Address List that you want to remove. The Source Address Lists details page appears.
4. Click the Delete Source Address List icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the Source Address List.
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 addresses. The GSS supports POSIX 1003.2-extended regular expressions when matching wildcards.

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.

This chapter contains the following major sections:

- Creating Domain Lists
- Modifying Domain Lists
- Deleting Domain Lists
- Where to Go Next

Creating Domain Lists

To create a domain list, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Domain Lists navigation link. The Domain Lists list page appears.
3. Click the Create Domain List icon. The Creating New Domain List details page appears.
4. In the General Configuration details page (General Configuration navigation link), perform the following:
   a. In the Name field, enter a name for the new domain list. Domain list names cannot contain spaces.
   b. From the Owner drop-down list, select the contact with whom the domain list will be associated.
   c. In the Comments text area, enter any comments for the new domain list.
5. Click the Add Domains navigation link to access the Add Domains section of the page. Use this section to add new hosted domains to your list.
6. In the space provided, enter the names of any hosted domains that you want to add to the domain 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.

Follow these guidelines when entering hosted domains:

- Hosted domains 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, separate each name with a semicolon as follows:
  - www.cisco.com; support.cisco.com; cdn.cisco.com

- The GSS supports domain names that use wildcards. The GSS supports POSIX 1003.2-extended regular expressions when matching wildcards. Any request for a hosted domain that matches the pattern is directed accordingly.

  For example, assume that you have 20 or more possible domains that the GSS is responsible, such as www1.cisco.com, www2.cisco.com, and so on. You can create a wildcard expression that covers all of those domains:
  - \*.cisco.com

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

7. Click the Add button. The GSS adds the specified domains to the domain list.

8. Click the General Configuration navigation link and view the domain list. The domain names appear under the Current Members section of the details page.

9. Click the Submit button to save your domain list changes and return to the Domain List lists page.

## Modifying Domain Lists

To modify an existing domain list, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Domain Lists navigation link. The Domain Lists list page appears.
3. From the Domain Lists list, click the Modify Domain List icon located to the left of the domain list that you want to modify. The Modifying Domain List details page appears.
4. In the General Configuration details page (General Configuration navigation link), use the fields provided to modify the name, comments, or owner for the domain list. Domain list names cannot contain spaces.
5. To add more domains to the list, click the Add Domains navigation link. Use the text box provided to enter the names of the domains that you want to add. Click the Add button to append the new domains to the existing list.
6. To remove the domains from the domain list, click the Remove Domains navigation link. The Remove Domains section of the page appears. Check the box accompanying each domain that you want to remove from the list, and then click the Remove Selected button. The GSS removes the deleted domain lists from the page.
7. Review your updated domain lists under the Current Members section of the details page.
8. Click the **Submit** button to save your changes and return to the Domain List list page.

### Deleting Domain Lists

You cannot delete domain lists associated with an existing DNS rule. Before deleting a domain list, verify that none of your DNS rules reference the domain list that you are about to delete. If necessary, deselect the domain 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 domain list from your GSS network, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Domain Lists** navigation link. The Domain Lists list page appears listing existing domain lists.
3. Click the **Modify Domain List** icon located to the left of the domain list that you want to remove. The Modifying Domain Lists details page appears.
4. Click the **Delete Domain List** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the domain list.

---

**Note**

If an error appears informing you that the domain list is referenced by a DNS rule, disassociate the domain list from the DNS rule and then attempt to delete the domain list again. See Chapter 7, Building and Modifying DNS Rules for more details.

5. Click **OK** to confirm your decision. You return to the Domain List list page.

### Where to Go Next

*Chapter 5, Configuring Keepalives*, describes the modification of global keepalives and the creation of shared 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 determine if a resource is online or offline.

The GSS uses keepalives to collect and track information on everything 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 SLBs and then uses this information to perform load-based redirection.

This chapter contains the following major sections:

- Modifying Global Keepalive Properties
- Configuring and Modifying Shared VIP Keepalives
- Where to Go Next

### 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 when no other keepalive values are specified. If required, you can modify the global keepalive properties for the GSS using the fields on the Global KeepAlive Properties details page (Resources tab). 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. If the GSS is transmitting numerous TCP keepalives using port 23, you should globally change the Number of Retries value for all TCP keepalives on the Configure Global KeepAlive Properties details page.

> **Note**
> Changing global keepalive properties is an optional process.

To modify the GSS keepalive properties, perform the following steps:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **KeepAlive Properties** navigation link. The Configure Global KeepAlive Properties details page appears.
3. Click the navigation links on the left side of the page to access the individual GSS global keepalive details page and to modify the global properties of the keepalive.

The following section describes how to modify the default properties for the individual global keepalives and contains the following topics:

- Globally Enabling or Disabling Keepalives
- Modifying ICMP Global Keepalive Settings
- Modifying TCP Global Keepalive Settings
- Modifying HTTP HEAD Global Keepalive Settings
- Modifying HTTPS 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

**Globally Enabling or Disabling Keepalives**

You can globally enable or disable keepalives of the type VIP, CRA, or Name Server. By default, all keepalive types are enabled.

The three types of possible keepalives on a GSS network are as follows:

- **VIP**—Virtual IP (VIP) addresses associated with an SLB such as the Cisco ACE, Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, Cisco Local Director, a web server, a cache, or any other geographically dispersed device in a global network deployment.
- **CRA**—Content routing agents that use a resolution process called DNS race to send identical and simultaneous responses back to user’s D-proxy.
- **Name Server**—Configured DNS name server that can answer queries that the GSS cannot resolve.

**Modifying ICMP Global Keepalive Settings**

To modify the ICMP global keepalive configuration settings, perform the following steps:

1. At the KAL Type section at the top of the page, choose either the Standard or Fast ICMP keepalive transmission rate to define the failure detection time for the GSS.

   The failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred and marks the answer offline.

   The Standard or Fast KAL-AP keepalive transmission rates are as follows:

   - **Standard**—Uses the default detection time of 60 seconds.
   - **Fast**—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 4 seconds.

   The GSS supports up to 750 ICMP keepalives when using the standard detection method and up to 150 ICMP keepalives when using the fast detection method.
2. If you chose the Standard KAL Type, in the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule ICMP keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

3. If you chose the Fast KAL Type, specify the following parameters:
   - In the Number of Retries field, specify the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. The default is 1.
   - In the Number of Successful Probes field, specify the number of consecutive successful ICMP 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 from 1 to 5 probes. The default is 1.

   Note: For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

4. Click the Submit button to save your ICMP global keepalive modifications.

Modifying TCP Global Keepalive Settings

To modify the TCP global keepalive global configuration settings, perform the following steps:

1. At the KAL Type section at the top of the page, choose either the Standard or Fast TCP keepalive transmission rate to define the failure detection time for the GSS.

   The failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred and marks the answer offline.

   The Standard or Fast KAL-AP keepalive transmission rates are as follows:
   - Standard—Uses the default detection time of 60 seconds.
   - Fast—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 4 seconds.

   Note: The GSS supports up to 1500 TCP keepalives when using the standard detection method and up to 150 TCP keepalives when using the fast detection method.

2. In the Destination port field, enter the port on the remote device that is to receive the TCP keepalive request from the GSS. The port range is from 1 to 65535. The default port is 80.

3. From the Connection Termination Method drop-down list, specify one of the following TCP keepalive connection termination methods:
   - Reset—The GSS immediately terminates the TCP connection by using a hard reset. This is the default termination method.
   - Graceful—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.
4. If you chose the Standard KAL Type, specify the following parameters:
   • In the Response Timeout field, specify the length of time allowed before the GSS retransmits data to a device that is not responding to a request. The valid entries are from 20 to 60 seconds. The default is 20 seconds.
   • In the Minimum Interval field, specify the minimum frequency with which the GSS attempts to schedule the TCP keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

5. If you chose the Fast KAL Type, modify the following parameters:
   • In the Number of Retries field, specify the number of times that the GSS retransmits a TCP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. The default is 1.

\[\text{Note}\] When using the Graceful termination sequence, there are two packets that require acknowledgement: SYN and FIN.

   • In the Number of Successful Probes field, specify the number of consecutive successful TCP 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 from 1 to 5 probes. The default is 1.

\[\text{Note}\] For more information on the keep alive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

6. Click the Submit button to save your TCP global keepalive modifications.

**Modifying HTTP HEAD Global Keepalive Settings**

To modify the HTTP HEAD keepalive global configuration settings, perform the following steps:

1. At the KAL Type section at the top of the page, choose either the Standard or Fast HTTP HEAD keepalive transmission rate to define the failure detection time for the GSS.

   The failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred and marks the answer offline.

   The Standard or Fast KAL-AP keepalive transmission rates are as follows:
   • Standard—Uses the default detection time of 60 seconds.
   • Fast—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 8 seconds.

\[\text{Note}\] The GSS supports up to 500 HTTP HEAD keepalives when using the standard detection method and up to 100 HTTP HEAD keepalives when using the fast detection method.

2. In the Destination port field, enter the port on the remote device that is to receive the HTTP HEAD-type keepalive request from the GSS. The port range is from 1 to 65535. The default port is 80.
3. In the Path field, enter the default path that is relative to the server website being queried in the HTTP HEAD request. For example: /company/owner

4. From the Connection Termination method drop-down list, specify one of these HTTP HEAD keepalive connection termination methods:
   - Reset—The GSS immediately terminates the HTTP HEAD connection by using a hard reset. This is the default termination method.
   - Graceful—The GSS initiates the graceful closing of a HTTP HEAD connection by using the standard three-way connection termination method.

   ![Caution](image)

   When using the graceful termination method and the server packets arrive at the GSS out of order (for example, the FIN packets arrive before the HTTP data), the GSS does not buffer or acknowledge receipt of the out-of-order packets and drops them. If the server does not retransmit the unacknowledged packets, the HTTP HEAD keepalive may place the answer in an offline state.

5. If you chose the Standard KAL Type, specify the following parameters:
   - In the Response Timeout field, change the length of time allowed before the GSS retransmits data to a device that is not responding to a request. The valid entries are from 20 to 60 seconds. The default is 20 seconds.
   - In the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule the HTTP HEAD keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

6. If you chose the Fast KAL Type, specify the following parameters:
   - In the Number of Retries field, specify the number of times that the GSS retransmits an HTTP HEAD packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. The default is 1.

   ![Note](image)

   When using the Graceful termination sequence, there are three packets that require acknowledgement: SYN, HEAD, and FIN.

   - In the Number of Successful Probes field, specify the number of consecutive successful HTTP HEAD 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 from 1 to 5 probes. The default is 1.

   ![Note](image)

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

7. Click the Submit button to save your HTTP HEAD global keepalive modifications.
Modifying HTTPS HEAD Global Keepalive Settings

To modify the HTTPS HEAD keepalive global configuration settings, perform the following steps:

1. **At the KAL Type section at the top of the page, choose either the Standard or Fast HTTPS HEAD keepalive transmission rate to define the failure detection time for the GSS. Failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred. This is the longest period of time the GSS will take to mark an answer offline. The GSS supports up to 500 HTTPS HEAD keepalives when using the standard detection method and up to 100 HTTPS HEAD keepalives when using the fast detection method.**

   The Standard or Fast HTTPS keepalive transmission rates are as follows:
   - Standard—Uses the default detection time of 60 seconds.
   - Fast—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 8 seconds.

2. **In the Destination port field, enter the port on the remote device that is to receive the HTTPS HEAD-type keepalive request from the GSS. The port range is 1 to 65535. The default port is 443.**

3. **In the Path field, enter the default path that is relative to the server website being queried in the HTTPS HEAD request.**

**Note**
The HTTPS path adheres to the RFC specification and is defined as follows:
https://<host>:<port>/<path>?<searchpart>; When you specify the path as blank (""), GSS sends the following URL: https://<host>:<port>/; When you specify the path as "index.html," GSS sends the following URL: https://<host>:<port>/index.html; When you specify the path as "/index.html," GSS sends the following URL: https://<host>:<port>\index.html.

4. **From the SSL Version drop down list, choose one of the following:**
   - SSLV2—Uses Secure Sockets Layer v2.
   - SSLV3—Uses Secure Sockets Layer v3.

5. **If you chose the Standard KAL Type, specify the following parameters:**
   - In the Response Timeout field, change 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 seconds.
   - In the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule HTTPS HEAD keepalives. The valid entries are 40 to 255 seconds. The default is 40 seconds.

6. **If you selected the Fast KAL type, in the Number of Successful Probes field, specify the number of consecutive successful HTTPS HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it into the GSS network). The range is 1 to 5 probes. The default is 1.**

**Note**
For Fast KAL Type, the number of times the GSS retransmits an HTTPS HEAD keepalive before declaring the device offline is internally fixed at 3. The interval between each attempt is fixed at 5 seconds, which results in a Calculated Transmission Interval of 20 seconds before the GSS declares a device offline. You cannot modify these settings.
7. Click the Submit button to save your changes.

Modifying KAL-AP Global Keepalive Settings

To modify the KAL-AP keepalive global configuration setting, perform the following steps:

1. At the KAL Type section at the top of the page, choose either the Standard or Fast KAL-AP keepalive transmission rate to define the failure detection time for the GSS.

   The failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred and marks the answer offline.

   The Standard or Fast KAL-AP keepalive transmission rates are as follows:
   - Standard—Uses the default detection time of 60 seconds.
   - Fast—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 4 seconds.

   Note: The GSS supports up to 128 primary and 128 secondary KAL-AP keepalives when using the standard detection method and up to 40 primary and 40 secondary KAL-AP keepalives when using the fast detection method.

2. If you intend to use Content and Application Peering Protocol (CAPP) encryption, in the CAPP Hash Secret field, enter an alphanumeric encryption key value. This alphanumeric value is used to encrypt interbox communications using CAPP. You must also configure the same encryption value on the Cisco ACE, CSS, or CSM. The default CAPP Hash Secret string is hash-not-set.

3. If you chose the Standard KAL Type, in the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule KAL-AP By Tag or KAL-AP By VIP keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

4. If you chose the Fast KAL Type, specify the following parameters:
   - In the Number of Retries field, specify the number of times that the GSS retransmits an KAL-AP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. The default is 1.
   - In the Number of Successful Probes field, specify 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 from 1 to 5 probes. The default is 1.

   Note: For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

5. Click the Submit button to save your KAL-AP global keepalive modifications.
Modifying Scripted Keepalive Global Keepalive Settings

To modify the Scripted keepalive global keepalive configuration settings, perform the following steps:

1. At the KAL Type section at the top of the page, choose either the Standard or Fast Scripted keepalive transmission rate to define the failure detection time for the GSS.

   The failure detection time is the amount of time between when a device failure occurs and when the GSS determines the failure occurred and marks the answer offline.

   The Standard or Fast Scripted keepalive transmission rates are as follows:
   - Standard—Uses the default detection time of 60 seconds.
   - Fast—Uses the user-selectable Number of Retries parameter to control the keepalive transmission rate. The default detection time is 24 seconds.

   \[\text{Note}\]
   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.

2. If you chose the Standard KAL Type, in the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule Scripted keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

3. If you chose the Fast KAL Type, specify the following parameters:
   - In the Number of Retries field, specify the number of times that the GSS retransmits a Scripted keepalive packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 5 retries. The default is 1.
   - In the Number of Successful Probes field, specify 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 from 1 to 5 probes. The default is 1.

   \[\text{Note}\]
   For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

4. Click the Submit button to save your Scripted keepalive global keepalive modifications.

Modifying CRA Global Keepalive Settings

To modify the Content Routing Agent (CRA) keepalive global configuration settings, perform the following steps:

1. In the Timing Decay field, change the value to specify how heavily the GSS should weigh recent DNS Round Trip Time (RTT) probe results relative to earlier RTT metrics, with 1 indicating that recent results should not be weighed any more than previous RTT results. The valid entries are from 1 to 10. The default is 2.
2. In the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule the CRA-type keepalives. The valid entries are from 1 to 60 seconds. The default is 10 seconds.

3. Click the **Submit** button to save your CRA global keepalive modifications.

## Modifying Name Server Global Keepalive Settings

To modify the Name Server keepalive global configuration settings, perform the following steps:

1. In the Query Domain field, change the globally defined domain name that is used to query when utilizing the name server (NS) keepalive. The default is ".".

2. In the Minimum Interval field, change the minimum frequency with which the GSS attempts to schedule the name server query keepalives. The valid entries are from 40 to 255 seconds. The default is 40 seconds.

3. Click the **Submit** button to save your Name Server global keepalive modifications.

## Configuring and Modifying 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 the 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 are an option for the ICMP, TCP, HTTP HEAD and HTTPS HEAD keepalive types.

This section contains the following topics:

- **Creating a Shared VIP Keepalive**
- **Configuring Scripted Keepalive Shared Keepalive Configuration Settings**
- **Deleting a Shared Keepalive**

## Creating a Shared VIP Keepalive

To create a shared VIP keepalive, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.

2. Click the **Shared KeepAlives** navigation link. The Shared KeepAlives list page appears listing all existing shared keepalives.
3. Click the **Create Shared KeepAlive** icon. The Creating New Shared KeepAlives details page appears.

4. At the Type section at the top of the page, choose from one of the five keepalive types as the shared VIP keepalive:
   - ICMP—Sends an ICMP echo message (ping) to the specified address. The online status is determined by the response received from the device and indicates simple connectivity to the network.
   - TCP—Sends a TCP handshake to the specified IP address and port number of the remote device to determine service viability (three-way handshake and connection termination method), and returns the online status of the device.
   - HTTP-Head—Sends a TCP format HTTP HEAD request to an origin web server at a specified address. The online status of the device is determined 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.
   - HTTPS-Head—Sends a TCP format HTTPS HEAD request to an origin Web server at a specified address. Online status of the device is determined in the form of an HTTPS Response Status Code of 200 (for example, HTTPS/1.0 200 OK) from the server as well as information on the Web page status and content size.
   - KAL-AP—Sends a detailed query to the Cisco ACE, CSS, or CSM to extract load and availability. The online status is determined when these SLBs respond with information about a hosted domain name, host VIP address, or a configured tag on a content rule.
   - Scripted Kal—Sends a detailed query that allows the GSS to use third-party applications to fetch load information from target devices.

This section describes how to configure the properties for the individual VIP-shared keepalives and contains the following sections:

- **Configuring ICMP Shared Keepalive Configuration Settings**
- **Configuring TCP Shared Keepalive Configuration Settings**
- **Configuring HTTP HEAD Shared Keepalive Configuration Settings**
- **Configuring HTTPS HEAD Shared Keepalive Configuration Settings**
- **Configuring KAL-AP Shared Keepalive Configuration Settings**
- **Configuring Scripted Keepalive Shared Keepalive Configuration Settings**

The default values used for each VIP keepalive is determined by the values specified in the Global Keepalive Properties details page.

---

**Configuring ICMP Shared Keepalive Configuration Settings**

To define the ICMP shared keepalive configuration, perform the following steps:

1. In the specified field, enter the IP address of the SLB that hosts the VIP. Both IPv4 and IPv6 IP addresses are supported.

2. If the ICMP global keepalive configuration is set to the Fast KAL Type, specify the following parameters in the Fast Keepalive Settings section:
   - In the Number of Retries field, specify the number of times that the GSS retransmits an ICMP echo request packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.

- In the Number of Successful Probes field, specify the number of consecutive successful ICMP 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 from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

Note: For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

3. Click the Submit button to save your ICMP shared keepalive configuration and return to the Shared KeepAlives list page.

Configuring TCP Shared Keepalive Configuration Settings

To define the TCP shared keepalive configuration, perform the following steps:

1. In the specified field, enter the IP address of the SLB that hosts the VIP. You can enter either an IPv4 or an IPv6 address.

2. In the Destination port field, enter the port on the remote device that is to receive the TCP keepalive request. The port range is from 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured value.

3. From the Termination Connection Method drop-down list, specify one of the TCP keepalive connection termination methods:
   - Global—Always use the globally defined TCP keepalive connection method.
   - Reset—The GSS immediately terminates the TCP connection by using a hard reset.
   - Graceful—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.

4. If the TCP global keepalive configuration is set to the Fast KAL Type, specify the following parameters in the Fast Keepalive Settings section:
   - In the Number of Retries field, specify the number of times that the GSS retransmits a TCP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.

Note: When using the Graceful termination sequence, there are two packets that require acknowledgement: SYN and FIN.

- In the Number of Successful Probes field, specify the number of consecutive successful TCP 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 from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.
Configuring HTTP HEAD Shared Keepalive Configuration Settings

To define the HTTP HEAD shared keepalive configuration, perform the following steps:

1. In the specified field, enter the IP address of the SLB that hosts the VIP. You can either enter an IPv4 or an IPv6 address in the IP Address field.

2. In the Destination port field, enter the port on the remote device that receives the HTTP HEAD-type keepalive request from the GSS. The valid entries are from 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured value.

3. In the Host Tag field, enter an optional domain name that is sent to the VIP as part of the HTTP HEAD query in the Host tag field. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.

4. In the Path field, enter the default 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. For example, enter:
   
   /company/owner

5. From the Connection Termination Method drop-down list, specify one of the HTTP keepalive connection termination methods:
   - Global—Always use the globally defined HTTP HEAD keepalive connection method.
   - Reset—The GSS immediately terminates the TCP formatted HTTP HEAD connection by using a hard reset.
   - Graceful—The GSS initiates the graceful closing of a TCP-formatted HTTP HEAD connection by using the standard three-way connection termination method.

   **Caution** When using the graceful termination method and the server packets arrive at the GSS out of order (for example, the FIN packets arrive before the HTTP data), the GSS does not buffer or acknowledge receipt of the out-of-order packets and drops them. If the server does not retransmit the unacknowledged packets, the HTTP HEAD shared keepalive may place the answer in an offline state.

6. If the HTTP HEAD global keepalive configuration is set to the Fast KAL Type, specify the following parameters in the Fast Keepalive Settings section:
   - In the Number of Retries field, specify the number of times that the GSS retransmits an HTTP HEAD packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.
Chapter 5  Configuring Keepalives

Configuring and Modifying Shared VIP Keepalives

### Configuring HTTPS HEAD Shared Keepalive Configuration Settings

To define the HTTPS HEAD shared keepalive configuration, perform the following steps:

1. In the specified field, enter the IP address used to test the online status for the linked VIPs. You can either enter an IPv4 or an IPv6 address in the IP Address field.

2. In the Destination port field enter the port on the remote device that receives the HTTPS HEAD-type keepalive request from the GSS. The port range is 1 to 65535. The default HTTP port is 443. If you do not specify a destination port, the GSS uses the globally configured value.

3. In the Host Tag field, enter an optional domain name that is sent to the VIP as part of the HTTPS HEAD query in the Host tag field. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.

4. In the Path field, enter the default path that is relative to the server website being queried in the HTTPS HEAD request. If you do not specify a default path, the GSS uses the globally configured value.

#### Note
The HTTPS path adheres to the RFC specification and is defined as follows:

- **https://<host>:<port>/**: When you specify the path as blank (""), GSS sends the following URL: `https://<host>:<port>/`
- **https://<host>:<port>/path**: When you specify the path as “index.html,” GSS sends the following URL: `https://<host>:<port>/index.html`
- **https://<host>:<port>/path?searchpart**: When you specify the path as “/index.html,” GSS sends the following URL: `https://<host>:<port>/index.html`

5. From the SSL Version drop down list, choose one of the following:
   - Global—Uses the global setting for SSL version (see Resources > Keepalive Properties > HTTPS Head).
   - SSLV2—Uses Secure Sockets Layer v2.
   - SSLV3—Uses Secure Sockets Layer v3.

6. For HTTPS HEAD keepalives of the type Fast, in the Number of Successful Probes field, specify the number of consecutive successful HTTPS HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online and reintroducing it into the GSS network.

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

7. Click the **Submit** button to save your HTTP HEAD shared keepalive configuration and return to the Shared KeepAlives list page.
network. This field appears only when the KAL Type attribute is set to Fast in the global HTTPS HEAD keepalive properties window (Resources > Keepalive Properties > HTTPS HEAD). The range is 1 to 5 probes. The default is 1.

Note For Fast KAL Type, the number of times the GSS retransmits an HTTPS HEAD keepalive before declaring the device offline is internally fixed at 3. The interval between each attempt is fixed at 5 seconds, which results in a Calculated Transmission Interval of 20 seconds before the GSS declares a device offline. You cannot modify these settings.

7. Click the Submit button to save your changes. You return to the Shared KeepAlives list page.

Configuring KAL-AP Shared Keepalive Configuration Settings

To define the KAL-AP shared keepalive configuration, perform the following steps:

1. Enter the primary (master) and secondary (backup) IP addresses of the SLBs that host the VIP. The secondary IP address is optional. The purpose of the secondary IP address is to query a second Cisco ACE, CSS, or CSM in a virtual IP (VIP) redundancy and virtual interface redundancy configuration.

Note You can use only IPv4 address for the primary and the secondary circuit IP addresses. The IPv6 addresses is not supported.

2. If you intend to use Content and Application Peering Protocol (CAPP) encryption, check the CAPP Secure box and enter an alphanumeric encryption key value in the CAPP Hash Secret field. This alphanumeric value is used to encrypt interbox communications using CAPP. You must also configure the same encryption value on the Cisco ACE, CSS, or CSM.

3. If the KAL-AP global keepalive configuration is set to the Fast KAL Type, specify the following parameters in the Fast Keepalive Settings section:

   • In the Number of Retries field, specify the number of times that the GSS retransmits an KAL-AP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.

   • In the Number of Successful Probes field, specify 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 from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

Note For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.

4. Click Submit to create the new KAL-AP shared keepalive and return to the Shared KeepAlives list page.
Configuring Scripted Keepalive Shared Keepalive Configuration Settings

To define the Scripted keepalive shared keepalive configuration, perform the following steps:

1. Enter the IP address of the SLB that hosts the VIP. You can either enter an IPv4 or an IPv6 address.
2. Enter the KAL name.
3. Choose the Scripted Kal Type. Options here include snmp-mib-not-index-by-vip, snmp-mib-index-by-vip, snmp-mib-scalar, CSS, CSM, or IOS-SLB.

Note: The ACE is not a Scripted Kal Type choice because a MIB/wrapper has not been implemented on the ACE to retrieve the VIP load value. An alternative is to use a KAL-AP shared keepalive (see the “Configuring KAL-AP Shared Keepalive Configuration Settings” section).

4. Enter the Community. The Community is the SNMP community name defined at the target device. The Community is the SNMP community name defined at the target device.

5. If the Scripted Kal Type is set to one of the non-Cisco SLBs, enter the Object Identifier (OID) and Address and Load filter types.

   The OID is the SNMP request sent for a specific community name. There are two types of OIDs: scalar and vector or table. For a scalar-type OID, the filter is not required, while for a vector-type, it is a requirement. It is useful in obtaining load information about some of the VIPs configured at the GSS.

6. You can choose one of the OID types: IpAddress or InetAddress.

   The IpAddress setting is for compatibility purposes with an older software release where the MIB structure supports the type as IpAddress and IPv4 IP address only. If you specify InetAddress, the MIB structure will be type InetAddress, and it supports both IPv4 and IPv6 addresses.

Table 5-1 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 5-1 have been tested and certified by Cisco Systems.

Table 5-1 MIBs, OIDs, and Filter IDs for Scripted Keepalive Types

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

* 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, (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.

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 because there is no table associated with the OID.

7. If the Scripted Kal global keepalive configuration is set to the Fast KAL Type, specify the following parameters in the Fast Keepalive Settings section:

- In the Number of Retries field, specify the number of times that the GSS retransmits a Scripted Kal request packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 5 retries. If you do not specify a value, the GSS uses the globally configured value.

- In the Number of Successful Probes field, specify 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 from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.
8. Click the Submit button to save your Scripted KAL shared keepalive configuration and return to the Shared KeepAlives list page.

Modifying a Shared Keepalive

To modify an existing shared keepalive, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Shared KeepAlives navigation link. The Shared KeepAlives list page appears.
3. Click the Modify Shared KeepAlive icon located to the left of the shared keepalive that you want to modify. The Modify Shared KeepAlive details page appears.
4. Use the fields provided to modify the shared keepalive configuration.
5. Click Submit to save your configuration changes and return to the Shared KeepAlive list page.

Deleting a Shared Keepalive

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. Use the procedure that follows to disassociate your answers and remove a shared keepalive from your GSS network.

⚠️ 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. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Shared KeepAlives navigation link. The Shared KeepAlives lists page appears listing all existing shared keepalives.
3. Click the Modify Shared KeepAlive icon located to the left of the shared keepalive that you want to remove. The Modifying Shared KeepAlive details page appears.
4. If the shared keepalive is associated with an answer, perform one of the following:
   - To disassociate all answers from the selected shared keepalive and set the keepalive type of each of those answers to ICMP using the answer’s own VIP, click the Set Answers KAL ICMP icon in the upper right corner of the page.
   - To disassociate all answers from the selected shared keepalive and set the keepalive type of each of those answers to none, which means that the GSS assumes they are always alive, click the Set Answers KAL None icon in the upper right corner of the page.

The GSS prompts you to confirm your decision to disassociate all the answers from the existing shared keepalive.
5. Click the Delete button in the upper right corner of the page. The GSS prompts you to confirm your decision to delete the shared keepalive.
6. Click OK to confirm your decision. You return to the Shared KeepAlives lists page.
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.
Chapter 6

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 and which can provide 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 a server load balancer (SLB) such as the Cisco CSS, Cisco CSM, Cisco ACE, Cisco IOS-compliant SLB, LocalDirector, a web server, cache, or other geographically dispersed SLBs 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 as resource pools, also referred to as answer groups. From the available answer groups, the GSS can use up to 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. Note that you can only configure 8K answers.

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.
Chapter 6      Configuring Answers and Answer Groups

Configuring and Modifying Answers

Note

The GSS does not delete the auto-configured IPv6 from its physical interface when you connect it to an interface with another device (for example, a Catalyst 6500 series switch) and change the prefix length on the switch interface. This might cause the keepalives to go off-line as the prefix length is deleted from the device that is connected to a GSS interface. Also, whenever the prefix change occurs in the interface device, you need to reload the GSS.

This section contains the following topics:

- Creating a VIP-Type Answer
- Creating a CRA-Type Answer
- Creating a Name Server-Type Answer
- Modifying an Answer
- Suspending an Answer
- Reactivating an Answer
- Suspending or Reactivating All Answers in a Location
- Deleting an Answer

Creating a VIP-Type Answer

The VIP-type answer refers to a virtual IP address (VIP) associated with an SLB device such as a Cisco CSS or CSM. When the GSS receives requests for content that is managed by an SLB, the GSS returns an A or AAAA record containing the VIP of the SLB that manages that content. The VIP IP address can either be an IPv4 or an IPv6 address.

When configuring a VIP-type answer, you have the option to configure one of a variety of different keepalive types or multiple keepalive types to test for that 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.

The primary GSSM allows you to assign multiple keepalives and 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, HTTPS 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.

Multiport keepalives enable the following applications:

- Monitor multiple ports on a server. For TCP or HTTP HEAD keepalives, you may also specify different destination ports. The multiport keepalive capability allows you to monitor a single server and check responses from multiple ports. If all of the keepalives in the VIP answer are successful, the GSS device considers the resource active and continues to redirect client traffic to the server. If just one of the keepalives fails, the GSS considers the answer offline and marks the server as unavailable. Subsequent successful connections to the server will reinstate it as an available resource.
- Monitor the status of an SLB device (such as a Cisco CSS, CSM, or ACE) and the various network connections to your servers. For this application, you configure the answer with a KAL-AP to monitor the ACE status. To monitor the network connections to the servers, you also configure the answer with multiple ICMP KALs (ping list).
Monitor both the status of an SLB device (such as a Cisco CSS, CSM, or ACE) and the status of a server. For this application, you configure the answer with a KAL-AP to monitor the SLB and retrieve the load value, and a Scripted keepalive to monitor the status (online or offline) of the server.

Use a KAL-AP keepalive and Scripted keepalive combination to perform the following operations:

- Globally load balance an SLB using KAL-AP.
- Check the performance of the back-end server cluster using Scripted keepalives if the back-end server cluster supports performance MIB objects. The Scripted keepalive uses the SNMP get request to fetch the load information from the target device.

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.

When configuring a multiport keepalive answer, observe the following rules:

- A multiport keepalive answer can contain one KAL-AP keepalive only.
- When using a combination of KAL-AP and Scripted keepalives, do not configure the Scripted keepalives for load enable. For this application, use the KAL-AP keepalive only to retrieve the load value. Use the Scripted keepalives to retrieve the status (online or offline) of the MIB object.

When the multiport keepalive answer is to contain multiple Scripted keepalives and no KAL-AP keepalive, configure only one Scripted keepalive for load enable to retrieve the load value. Configure the remaining Scripted keepalives for device status retrieval only.

Once an answer is created, you cannot modify the answer type (for example, from VIP to CRA).

The IPv4 and IPv6 VIP answers can co-exist in the same VIP answer group.

To configure a VIP-type answer, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answers navigation link. The Answers list page appears.
3. Click the Create Answer icon. The Creating New Answer details page appears.
4. In the Type field, click the VIP option button. The VIP Answer section appears in the details page.
5. (Optional) In the Name field, enter a name for the VIP-type answer that you are creating.
6. From the Location drop-down list, choose a GSS location that corresponds to the answer. Specifying a location for an answer is an optional step unless you are assigning a location that is associated with a proximity zone to the answer. For details about creating a location, see Chapter 2, Configuring Resources.
7. (Optional) Check the Manual Reactivation checkbox to enable this function for the answer. When enabled, the GSS suspends the answer if it goes offline and changes its status to “operational suspend.” The answer remains suspended until you reactivate it. When not enabled, the GSS automatically reverts to using the answer when it returns to an online state.

If you enable the manual reactivate function for an answer, you must also enable the global manual reactivate function for it to work (see the “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8).
8. In the VIP address field, enter the VIP address to which the GSS will forward requests. You can either enter an IPv4 or an IPv6 address as the VIP address.

9. In the VIP Keepalive section, check the **Multi-port** check box if you want to enable the selection of multiple keepalives and destination ports for the VIP-type answer. Leave this check box unchecked if you intend to configure a VIP-type answer that is to support only one keepalive type to test for the answer.

The Multi-port icon appears to the right of the Multi-port check box, while the Multi-port Keepalive section appears at the bottom of the Creating New Answer details page.

The Multi-port Keepalive section contains the following:

- A VIP Address checkbox that allows you to choose either a shared or nonshared keepalive (a checked box specifies a nonshared keepalive, while an unchecked box specifies a shared keepalive).
- An IP Address field that allows you to specify the IP address (IPv4 or IPv6) of the device to be monitored by the keepalive. This field is accessible only when configuring nonshared keepalives (the VIP Address checkbox must be checked).

To add additional keepalives or destination ports for the VIP-type answer, click the **Multi-port** icon. The primary GSSM GUI adds a new numbered keepalive section to the bottom of the Creating New Answer details page.

The primary GSSM allows you to configure keepalives that specify the IP addresses of multiple devices on your network, as well as configure multiple shared keepalives. The primary GSSM supports a maximum of five keepalives for a VIP answer.

To remove a keepalive from the Creating New Answer details page, click the **Remove** check box associated with a specific keepalive.

10. Choose from one of these seven keepalive types for your VIP answer:

- **None**—Does not send keepalive queries to the VIP. The GSS assumes that the VIP is always alive. The None selection is supported only in single keepalive mode.
- **ICMP**—Sends an ICMP echo message (ping) to the specified address. The GSS determines the online status by the response received from the device, indicating simple connectivity to the network.
- **TCP**—Sends a TCP handshake to the specified IP address 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.
- **HTTP HEAD**—Sends a TCP-format HTTP HEAD request to an origin web server at a specified address. 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.
- **HTTPS HEAD**—Sends a TCP format HTTPS HEAD request to an origin Web server at a specified address. Online status of the device is determined in the form of an HTTPS Response Status Code of 200 (for example, HTTPS/1.0 200 OK) from the server as well as information on the Web page status and content size.
- **KAL-AP**—Sends a detailed query to the Cisco CSS or CSM to extract 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 KAL-AP selection is supported only for the first keepalive in multi-port keepalive mode. Note that only IPv4 is supported.
• SCRIPTED-Kal—Sends a detailed query that allows the GSS to use third-party applications to
fetch load information from target devices.

Table 6-1 describes the combinations for the VIP Address field and keepalive addresses.

<table>
<thead>
<tr>
<th>VIP Address</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: KAL-AP Keepalive supports only IPv4.

This section describes how to configure the properties for the individual VIP keepalives and contains the
following topics:
• Configuring ICMP Keepalive VIP Answer Settings
• Configuring TCP Keepalive VIP Answer Settings
• Configuring HTTP HEAD Keepalive VIP Answer Settings
• Configuring HTTPS HEAD Keepalive VIP Answer Settings
• Configuring KAL-AP Keepalive VIP Answer Settings
• Configuring Scripted Keepalive VIP Answer Settings

Note: The default values used for each of the VIP keepalives are determined by the values specified in the
Global Keepalive Properties details page.

Configuring ICMP Keepalive VIP Answer Settings

To define the shared ICMP keepalive for your VIP answer, perform the following steps:

1. Uncheck the VIP Address check box and choose an ICMP-type shared keepalive from the Shared
ICMP Keepalive drop-down list. The VIP Address check box is automatically checked to instruct
the GSS to send an ICMP echo message (ping) to the VIP address of the remote device and
determine the online status.

2. If the ICMP global keepalive configuration is set to the Fast KAL Type and the VIP Address is
checked, specify the following parameters in the Fast Keepalive Settings section:
   • In the Number of Retries field, specify the number of times that the GSS retransmits an ICMP
     echo request packet before declaring the device offline. As you adjust the Number of Retries
     parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally
     configured value.
• In the Number of Successful Probes field, specify the number of consecutive successful ICMP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it back into the GSS network). The valid entries are from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

**Note** For more information on the keepalive detection time, see Chapter 1, Introducing the Global Site Selector, the “Keepalives” section.

3. Click the **Submit** button to save your ICMP keepalive VIP answer and return to the Answers list page.

### Configuring TCP Keepalive VIP Answer Settings

To define the shared TCP keepalive for your VIP answer, perform the following steps:

1. Uncheck the VIP Address check box and choose a TCP-type shared keepalive from the Shared TCP Keepalive drop-down list. The VIP Address check box is automatically checked to instruct the GSS to send a TCP keepalive to the VIP address of the remote device and determine online status.

2. In the Destination Port field, enter the port on the remote device that is to receive the TCP keepalive request. The valid entries are from 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured value.

3. If you enabled the VIP Address check box, specify one of the TCP keepalive connection termination methods:
   - Global—Always use the globally defined TCP keepalive connection method.
   - Reset—The GSS immediately terminates the TCP connection by using a hard reset.
   - Graceful—The GSS initiates the graceful closing of a TCP connection by using the standard three-way connection termination method.

4. If the TCP global keepalive configuration is set to the Fast KAL Type and the VIP Address is checked, specify the following parameters in the Fast Keepalive Settings section:
   • In the Number of Retries field, specify the number of times that the GSS retransmits a TCP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.

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

• In the Number of Successful Probes field, specify the number of consecutive successful TCP keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it back into the GSS network). The valid entries are from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

**Note** For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.
5. Click the **Submit** button to save your TCP keepalive VIP answer and return to the Answers list page.

### Configuring HTTP HEAD Keepalive VIP Answer Settings

To define the shared HTTP HEAD keepalive for your VIP answer, perform the following steps:

1. Uncheck the VIP Address check box and choose an HTTP-type shared keepalive from the Shared HTTP HEAD keepalive drop-down list. The VIP Address check box is automatically checked to instruct the GSS to send a TCP-format HTTP HEAD request to the web server at an address you specified and determine online status.

2. In the Destination Port field, enter the port on the remote device that receives the HTTP HEAD-type keepalive request from the GSS. The valid entries are from 1 to 65535. If you do not specify a destination port, the GSS uses the globally configured value.

3. In the Host Tag field, enter an optional domain name that is sent to the VIP as part of the HTTP HEAD query in the Host tag field. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.

4. In the Path field, enter 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. For example, enter:

```
/company/owner
```

5. If you enabled the VIP Address check box, specify one of the HTTP HEAD keepalive connection termination methods:

   - Global—Always use the globally defined HTTP HEAD keepalive connection method.
   - Reset—The GSS immediately terminates the TCP-formatted HTTP HEAD connection by using a hard reset.
   - Graceful—The GSS initiates the graceful closing of a TCP-formatted HTTP HEAD connection by using the standard three-way connection termination method.

6. If the HTTP HEAD global keepalive configuration is set to the Fast KAL Type and the VIP Address is checked, specify the following parameters in the Fast Keepalive Settings section:

   - In the Number of Retries field, specify the number of times that the GSS retransmits a TCP packet before declaring the device offline. As you adjust the Number of Retries parameter, 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 from 1 to 10 retries. If you do not specify a value, the GSS uses the globally configured value.

   - **Note** When using the Graceful termination sequence, three packets require acknowledgement: SYN, HEAD, and FIN.

   - In the Number of Successful Probes field, specify the number of consecutive successful HTTP HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it back into the GSS network). The valid entries are from 1 to 5 probes. If you do not specify a value, the GSS uses the globally configured value.

   - **Note** For more information on the keepalive detection time, see the “Keepalives” section in Chapter 1, Introducing the Global Site Selector.
7. Click the **Submit** button to save your HTTP HEAD keepalive VIP answer and return to the Answers list page.

### Configuring HTTPS HEAD Keepalive VIP Answer Settings

To define the shared HTTPS HEAD keepalive for your VIP answer, perform the following steps:

1. The VIP Address check box is automatically checked to instruct the GSS to send a TCP format HTTPS HEAD request to the web server at an address you specified and determine online status. If necessary, uncheck the VIP Address check box and select an HTTPS-type shared keepalive from the Shared HTTPS HEAD keepalive drop-down list.

2. In the Host Tag field, enter an optional domain name that is sent to the VIP as part of the HTTPS HEAD query in the Host tag field. This tag allows an SLB to resolve the keepalive request to a particular website even when multiple sites are represented by the same VIP.

3. In the Destination port field enter the port on the remote device that receives the HTTPS HEAD-type keepalive request from the GSS. The port range is 1 to 65535. The default HTTPS port is 443. If you do not specify a destination port, the GSS uses the globally configured value.

4. In the IP Address field, enter the IP address of the remote device that receives the HTTPS HEAD keepalive request from the GSS. Enter an IP address in this field only when the address is different than the VIP address that you specified in the VIP Answer section.

5. In the Path field, enter the default path that is relative to the server website being queried in the HTTPS HEAD request. If you do not specify a default path, the GSS uses the globally configured value.

6. From the SSL Version drop-down list, choose one of the following:
   - Global - Uses the global setting for SSL version (see Resources > Keepalive Properties > HTTPS Head).
   - SSLV2 - Uses Secure Sockets Layer v2.
   - SSLV3 - Uses Secure Sockets Layer v3.

7. If you selected the Fast KAL type, in the Number of Successful Probes field, specify the number of consecutive successful HTTPS HEAD keepalive attempts (probes) that must be recognized by the GSS before bringing an answer back online (and reintroducing it into the GSS network). The range is 1 to 5 probes. The default is 1.

8. Click the **Submit** button to save your changes. You return to the Answers list page.

---

**Note**

The HTTPS path adheres to the RFC specification and is defined as follows:

- `https://<host>:<port>/ <path>?<searchpart>`: When you specify the path as blank (""), GSS sends the following URL: `https://<host>:<port>/`.

---

**Note**

For Fast KAL type, the number of times the GSS retransmits an HTTPS HEAD keepalive before declaring the device offline is internally fixed at 3. The interval between each attempt is fixed at 5 seconds, which results in a Calculated Transmission Interval of 20 seconds before the GSS declares a device offline. You cannot modify these settings.
Configuring KAL-AP Keepalive VIP Answer Settings

Note  You can use only IPv4 address for the primary and the secondary circuit IP addresses. The IPv6 addresses is not supported.

To define the shared KAL-AP keepalive for your VIP answer, perform the following steps:

1. From the KAL-AP Type drop-down list, select one of the following formats of the KAL-AP keepalive query:
   - KAL-AP By Tag—Embeds 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 confusion that can be caused when probing for the status of a VIP that is located behind a firewall network address translation (NAT). The Tag IP address can only be IPv4 IP address.
   - KAL-AP By VIP—Embeds the keepalive VIP address in the KAL-AP request. The KAL-AP queries the keepalive address to determine the online status. The VIP IP address can only be an IPv4 address.

   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. This results in the dropped datagram not getting updated load values on the VIPs that expect them. This situation 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.

   To resolve this behavior, use the KAL-AP by VIP format 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 KAL-AP by Tag format. However, you must limit the length of Tag Names to ensure that the packets do not exceed 1.4 K.

2. If you chose KAL-AP By VIP, choose the appropriate KAL-AP type keepalive from the Shared KAL-AP Keepalive drop-down list.

3. If you chose KAL-AP By Tag, choose the appropriate KAL-AP type keepalive from the Shared KAL-AP Keepalive drop-down list, and then enter a unique alphanumeric value in the Tag field. This value is used as a “key” by the CSS or GSSM that matches the KAL-AP request with the appropriate VIP.

4. Click the Submit button to save your KAL-AP keepalive VIP answer and return to the Answers list page.

Configuring Scripted Keepalive VIP Answer Settings

To define the shared Scripted keepalive for your VIP answer, perform the following steps:

1. From the Shared Scripted KeepAlive drop-down list, select a Scripted keepalive.

2. Enter the Max VIP load in the specified field.

Note  For more information on the keepalive detection time, see Chapter 1, Introducing the Global Site Selector, the “Keepalives” section.
3. Click the **Submit** button to save your Scripted keepalive VIP answer and return to the Answers list page.

### Creating 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.

**Note**

Once an answer is created, you cannot modify the answer type (for example, from CRA to VIP).

**Note**

You can configure CRA-type answer type, by using only an IPv4 address.

To configure a CRA-type answer type, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears.
3. Click the **Create Answer** icon. The Creating New Answer details page appears.
4. In the Type selection field, click the **CRA** option button. The CRA Answer section appears in the details page.
5. (Optional) In the Name field, enter a name for the CRA-type answer.
6. (Optional) In the Location drop-down list, choose a location for the answer. Ensure that the name is unique. For details about creating a location, see Chapter 2, Configuring Resources.
7. (Optional) Check the Manual Reactivation check box to enable this function for the answer. When enabled, the GSS suspends the answer if it goes offline and changes its status to “operational suspend.” The answer remains suspended until you reactivate it. When not enabled, the GSS automatically reverts to using the answer when it returns to an online state.

**Note**

If you enable the manual reactivate function for an answer, you must also enable the global manual reactivate function for it to work (see the “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8).

8. In the CRA Address field, enter the interface or circuit address of the CRA.
9. If you want the GSS to perform keepalive checks on the CRA-type answer, click the **Perform KeepAlive Check** check box. Uncheck the Perform KeepAlive option if a static one-way delay value is used.

10. If you require a one-way delay time, enter a value, in milliseconds, in the One Way Delay field. 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.

11. Click **Submit** to create your new CRA-type answer and return to the Answers list page.

---

### Creating 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.

---

**Note**

Once an answer is created, you cannot modify the answer type (for example, from name server to VIP).

**Note**

You can configure Name Server-type answer type, by using only an IPv4 address.

To configure a name server-type answer, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears.
3. Click the **Create Answer** icon. The Creating New Answer details page appears.
4. In the Type field, click the **Name Server** option button. The Name Server Answer section appears in the Creating New Answer details page.
5. (Optional) In the Name field, enter a name for the name server-type answer.
6. (Optional) From the Location drop-down list, choose a GSS location to which the answer corresponds. For details about creating a location, see Chapter 2, Configuring Resources.
7. (Optional) Check the Manual Reactivation checkbox to enable this function for the answer. When enabled, the GSS suspends the answer if it goes offline and changes its status to “operational suspend.” The answer remains suspended until you reactivate it. When not enabled, the GSS automatically reverts to using the answer when it returns to an online state.

**Note**

If you enable the manual reactivate function for an answer, you must also enable the global manual reactivate function for it to work (see the “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8).

8. In the Name Server Address field, enter the IP address of the name server that the GSS is to forward its requests.
9. If you want the GSS to perform keepalive checks on the specified Name Server, click the Perform KeepAlive Check check box. The GSS queries the specified name server address to determine the online status.

10. If you want to have the GSS query the name server for a specific domain in determining the online status, enter the domain name in the KeepAlive Query Domain field.

   If no domain is specified, the GSS queries the default query domain. For instructions on configuring the default query domain, see Chapter 5, Configuring Keepalives.

11. Click Submit to create your new name server-type answer and return to the Answers list page.

Modifying an Answer

Once you have configured your answers, they can be modified at any time. However, once an answer is created, you cannot modify the answer type (for example, from VIP to CRA).

Note

If you have the manual reactivation function enabled for the answer and the GSS has the answer operationally suspended, modifying the answer will reactivate it.

To modify an existing answer, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answers navigation link. The Answers list page appears.
3. Click the Modify Answer icon located to the left of the answer that you want to modify. The Modifying Answer details page appears.
4. Use the fields provided to modify the answer configuration.
5. Click Submit to save your configuration changes and return to the Answers list page.

Suspending an Answer

To temporarily stop the GSS from using an active answer, use the Suspend Answer icon on the Modifying Answer details page. It 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 from the Modify Answer Group details page. See the “Suspending or Reactivating Answers in an Answer Group” section for details.

To suspend an answer from the Modify Answer details page, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answers navigation link. The Answers list page appears.
3. Click the Modify Answer icon located to the left of the answer that you want to suspend. The Modifying Answer details page appears.
4. Click the Suspend Answer icon in the upper right corner of the page to suspend an answer.
5. Click OK to confirm your decision and return to the Answers list screen. The modified answer has a status of “Suspended.”
To reactivate a suspended answer, use the activate feature (see the “Reactivating an Answer” section).

Reactivating an Answer

To reactivate a suspended answer from the Modify Answer details page, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answers navigation link. The Answers list page appears.
3. Click the Modify Answer icon located to the left of the answer that you want to activate. All suspended answers have a status of “Suspended” in the list. The Modifying Answer details page appears.
4. Click the Activate Answer icon in the upper right corner of the page to reactivate an answer.
5. Click OK to confirm your decision and return to the Answers list screen. The modified answer has a status of “Active.”

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 for software upgrades or regular maintenance.

The GSS automatically detects and routes requests around suspended answers. Manually 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, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click the Modify Location icon located to the left of the location that includes answers that you want to suspend or reactivate. The Modifying Location details page appears.
4. Perform one of the following:
   - To suspend answers associated with this location, click the Suspend All Answers in This Location icon.
   - To reactivate manually suspended answers associated with this location, click the Activate All Answers in This Location icon.

Note Reactivating all location answers reactivates only the answers that you suspended. If the manual reactivation function is enabled on the answer and the GSS operationally suspended the answer, it will remain operationally suspended. To reactivate operationally suspended answers, see “Activating All Operationally Suspended Answers or Clauses” section on page 2-9

5. Confirm your decision to suspend or activate the answers associated with this location.
6. Click OK to confirm your decision and return to the Locations list page.
Deleting an Answer

If you have created an answer but want to delete it from the GSS, use the delete feature on the primary GSSM GUI to remove that 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. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answers navigation link. The Answers list page appears.
3. Click the Modify Answer icon located to the left of the answer that you want to remove. The Modifying Answer details page appears.
4. Click the Delete Answer icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the answer.
5. Click OK to confirm your decision and return to the Answers list page.

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 a particular balance method that is used to resolve the request as follows:

- 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 up to 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
- Configuring an Authority Domain for an Answer Group
- Deleting an Authority Domain for an Answer Group
- Suspending or Reactivating Answers in an Answer Group
- Suspending or Reactivating All Answers in an Answer Group Associated with an Owner
- Deleting an Answer Group
Creating an Answer Group

You can configure up to 4000 answer groups on the primary GSSM. To create an answer group, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answer Groups navigation link. The Answer Groups list page appears.
3. Click the **Create Answer Group** icon. The Creating New Answer Group details page appears.

4. In the General Configuration details page (**General Configuration** navigation link), perform the following:
   - In the Name field, enter a name for the new answer group. The answer group name cannot contain spaces.
   - From the Type drop-down list, choose one of the following three options:
     - Name Server—The answer group consists of configured name servers.
     - CRA—The answer group consists of content routing agents (CRAs) for use with the boomerang server component of the GSS.
     - VIP—The answer group consists of virtual IPs controlled by an SLB device such as a CSS or CSM.

   Note that the maximum number of answers that you can place in each of these answer groups is 20 for a CRA answer group, 30 for an NS answer group, and 100 for a VIP answer group. You can add IPv4 or IPv6 answers to the same answer group.

5. From the Owner drop-down list, choose the GSS owner with which the answer group will be associated. For details about creating an owner, see Chapter 2, Configuring Resources.

6. In the Comments text area, enter a description or other instructions regarding the new answer group.

7. Click the **Add Answers** navigation link to access the Add Answers section of the page. Perform the following:
   a. Click the check box corresponding to each answer that you wish to add to the answer group. If the list of answers on your GSS network spans more than one page, choose the answers from only the first page of answers and proceed to the next step.

   **Note**
   You can add both IPv4 and IPv6 address in the same answer group.

   b. Click the **Add Selected** button. The GSS adds the selected answers to the answer group. Answers can belong to more than one answer group simultaneously.

   c. Repeat Steps a and b if your answers span multiple pages.

   **Note**
   If an answer is added to multiple answer groups, when you view the hit count of answers from either the Answer Status list page or the **show statistics dns** CLI command output, the number of hits provided represents the aggregate number of hits for that answer across all answer groups.

8. Click the **General Configuration** navigation link to return to the General Configuration section. The newly added answers appear in the Current Members section. There are different configuration options depending on the type of answer group.

9. Perform one of the following:
   - If configuring CRA, no configuration parameters are required.
   - If configuring a Name Server type answer group, assign an order and weight to each Answer in the answer group using the field and drop-down list provided.
Note: To configure the CRA and Name Server use only the IPv4 IP address. The IPv6 address is not supported.

- If configuring a VIP type answer group, assign an order, load threshold (LT), and weight to each answer in the answer group using the fields and drop-down lists provided.

Note: Load thresholds, which allow the GSS to make routing decisions based on how heavily a particular resource is being tasked, can only be assigned to VIP answers using a KAL-AP keepalive.

For more information on the order, weight, and load threshold settings, see the “Balance Methods” section in Chapter 1, Introducing the Global Site Selector.

10. Click the Submit button to save your answer group and return to the Answer Group list page.

Modifying an Answer Group

Once you create your answer groups, use the primary GSSM GUI 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. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answer Groups navigation link. The Answer Groups list page appears.
3. Click the Modify Answer Group icon located to the left of the answer group that you want to modify. The Modify Answer Group details page appears.
4. In the General Configuration details page (General Configuration navigation link), use the fields provided to modify the name, owner, or comments for the answer group.
5. Click the Add Answers navigation link. Click the check box corresponding to each answer that you want to add to the answer group. If the list of answers on your GSS network spans more than one page, choose the answers from only the first page of answers, and then click Add Selected, before proceeding to another page of answers.
6. To remove answers from the answer group, click the Remove Answers navigation link. The Remove Answers section of the page appears. Click the check box accompanying each answer that you want to remove from the list, and then click the Remove Selected button. The GSS removes the selected answers from the page.
7. Review your updated answer group under the Current Members section of the General Configuration details page.
8. Click the Submit button to save your changes and return to the Answer Groups Lists page.
Chapter 6 Configuring Answers and Answer Groups

Configuring an Authority Domain for an Answer Group

As detailed in Chapter 1, 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 it 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 an authority domain for an answer group, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears.
3. Click the **Create Answer Group** button and create a new answer group named NSG1 of type Name Server.
4. Click **Submit** to save your configuration changes and return to the Answer Groups list page.
5. Click the **Modify Answer Group** icon located to the left of the NSG1 answer group. The Modify Answer Group details page appears.
6. Click the **Add Auth-Domains** navigation link.
7. Enter example.com and then click **Add** to add your new Auth-Domain to the list.
   A message appears at the bottom of the screen indicating that 1 auth-domain has been successfully added to the group.
8. Click **Submit** to save your configuration changes and return to the Answer Groups list page.
9. Click the **Modify Answer Group** icon located to the left of the NSG1 answer group once more. The revised Modify Answer Group details page appears with the new Auth-Domain member, example.com.

Deleting an Authority Domain for an Answer Group

To delete an authority domain for an answer group, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears.
3. Click the **Modify Answer Group** icon located to the left of the answer group that you want to remove. The Modifying Answer Group details page appears.
4. Click the **Remove Auth-Domains** navigation link. The Remove Auth-Domains details page appears.
5. Click the **Remove** selection box in the upper-left corner, and then click the **Remove Selected** button.
   A message appears at the bottom of the screen indicating that 1 auth-domain has been successfully removed from the group.
6. Click the **Submit** button to save your changes and return to the Answer Groups Lists page.
Suspending or Reactivating Answers in an Answer Group

You can temporarily stop the GSS from directing requests to it by using the Suspend Answers icon on the primary GSSM GUI. The Suspend Answers function temporarily suspends the answers that make up that group and prevents the answer group from being used by any of the currently configured DNS rules. You can suspend all answers associated with the answer group or suspend individual answers in the group.

Use the Activate Answers icon to reactivate the answers in the answer group.

Note

Suspending the answers in one answer group also affects any other answer groups to which those answers belong.

To suspend or reactivate answers in an answer group, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Answer Groups navigation link. The Answer Groups list page appears.
3. Click the Modify Answer Group icon located to the left of the answer group that you want to suspend or reactivate. The Modifying Answer Group details page appears.
4. Perform one of the following steps to suspend answers in the answer group:
   - To suspend all answers in the answer group, click the Suspend Answers icon in the upper-right corner of the page.
   - To suspend individual answers associated with the answer group, click the Suspend Answer icon to the right of the answer in the General Configuration details page.
5. Perform one of the following steps to reactivate suspended answers in the answer group:
   - To reactivate all answers in the answer group, click the Activate Answers icon in the upper-right corner of the page.
   - To reactivate individual answers associated with the answer group, click the Activate Answer icon to the right of the answer in the General Configuration details page.
6. Click OK to confirm your decision and return to the Answer Groups list page.

To view the status of the suspended or activated answers, see Chapter 11, Monitoring GSS Global Server Load-Balancing Operation.

Suspending or Reactivating All Answers in an Answer Group 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 simplifies the process to quickly suspend or activate related answers.

To suspend or reactivate all answers in answer groups associated with a GSS owner, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Owners navigation link. The Owners list page appears.
3. Click the Modify Owner icon located to the left of the answer group that you want to suspend or reactivate. The Modifying Owner details page appears.
4. Perform one of the following steps:
   - To suspend all answers in all answer groups associated with this owner, click the **Suspend All Answers in All Groups for This Owner** icon in the upper-right corner of the details page.
   - To reactivate all suspended answers associated with this owner, click the **Activate All Answers in All Groups for This Owner** icon in the upper-right corner of the details page.

5. Click **OK** to confirm your decision to suspend or activate the answers. You return to the Owner list page.

### Deleting an Answer Group

You can delete an answer group from the GSS by using the Delete Answer Group icon on the primary GSSM GUI to remove that answer group. 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.

---

**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 group, perform one of the following steps:

1. From the primary GSSM GUI, click **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears.
3. Click the **Modify Answer Group** icon located to the left of the answer group that you want to remove. The Modifying Answer Group details page appears.
4. Click the **Delete Answer Group** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the answer group.
5. Click **OK** to confirm your decision and return to the Answer Groups list page.

---

### 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.
CHAPTER 7

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.

Before you create DNS rules, see the “GSS Architecture” section in Chapter 1, Introducing the Global Site Selector.

This chapter contains the following major sections:

- DNS Rule Configuration Overview
- Building DNS Rules Using the Wizard
- Building DNS Rules Using the DNS Rule Builder
- Modifying DNS Rules
- Suspending a Clause
- Reactivating a Clause
- Reactivating Operationally Suspended Clauses
- 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
DNS Rule Configuration Overview

Because of the complexity of DNS rules, the primary GSSM GUI provides you with a choice of two methods for creating a DNS rule:

- DNS Rule Wizard
- DNS Rule Builder

Both of these topics are explained in the sections that follow.

DNS Rule Wizard

The DNS Rule Wizard guides you through the process of creating a DNS rule. The DNS Rule Wizard allows you to create source address lists, domain lists, answer groups, and balance methods as required. Owners, regions, and locations are not created as part of the DNS Rule Wizard, however. Instead, you must create them before using the wizard.

The DNS sticky and network proximity global server load-balancing applications are configurable only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable DNS sticky, proximity, or the manual reactivation function (see “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8) in a DNS rule.

When you use the wizard, click the Next and Back buttons to move you forward and backward through the rule-building process. Alternatively, you can click the navigation links under the Wizard Contents heading to move between any step in the wizard.

To access the DNS Rule Wizard, perform the following steps:

1. Click the DNS Rules tab.
2. Click the Rule Wizard icon.

See the “Building DNS Rules Using the Wizard” section for details.

DNS Rule Builder

You can use the DNS Rule Builder to quickly assemble DNS rules from source address lists, domain lists, owners, and answers that you have already created. By using the available fields and drop-down menus, you can assign a name for your rule and then configure the rule with up to three balance clauses for the GSS to choose an answer.

The balance clauses that you configure in a DNS rule are evaluated in order. Parameters are established to determine when a clause is skipped and the next clause is used. A balance clause is skipped when any one of the following conditions exits:

- The 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 Director Response Protocol (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.
The DNS Rule Builder pulls together all the GSS elements needed to create new DNS rules. The DNS Rule Builder is launched in its own window, which enables you to leave it open and return to the primary GSSM GUI to review or add answers, answer groups, owners, domain lists, and more. Any changes made to your GSS network configuration while the DNS Rule Builder is open are immediately reflected in the DNS Rule Builder. For example, an answer group added while the DNS Rule Builder window is open automatically appears in the drop-down list of answer groups.

In addition, the DNS Rule Builder allows you to configure multiple clauses for your DNS rule; that is, you can configure additional answer group and balance method pairs that can be tried if the first answer group and balance method specified does not yield an answer.

To access the DNS Rule Builder, perform the following steps:

1. Click the DNS Rules tab.
2. Click the Open Rule Builder icon.

See the “Building DNS Rules Using the DNS Rule Builder” section for details.

---

### Building DNS Rules Using the Wizard

To create a DNS rule using the DNS Rule Wizard:

1. From the primary GSSM GUI, click the DNS Rules tab and then the DNS Rules navigation link. The DNS Rules list appears.
2. Click the Rule Wizard icon. The DNS Rule Wizard introduction page appears. This page provides an overview of the steps necessary to create a DNS rule.
3. Click the Next and Back buttons to move through the DNS rule-building process. Alternatively, you can click the links under the Wizard Contents table of contents to move between steps in the Wizard.

This section describes how to configure the properties for the individual pages in the DNS Rule Wizard. It contains the following topics:

- Identifying a Source Address List in the DNS Rule Wizard
- Specifying a Domain List in the DNS Rule Wizard
- Configuring an Answer Group in the DNS Rule Wizard
- Choosing a Balance Method in the DNS Rule Wizard
- Reviewing the Summary Page in the DNS Rule Wizard
### Identifying a Source Address List in the DNS Rule Wizard

The Source Address List section of the DNS Rule Wizard allows you to identify a source address list, which is a list of address blocks that identify DNS proxies.

To identify a source address list in the DNS Rule Wizard, perform the following steps:

1. Perform one of the following actions:
   - To apply the DNS rule to requests originating from any DNS proxy, click the **Any Address** option, and then click **Next**. See the “Specifying a Domain List in the DNS Rule Wizard” section for information on using the Domain List detail page in the wizard.
   - To apply the DNS Rule to requests originating from a list of DNS proxies that you want to configure, click **Manually-entered source address list**, and then click **Next**. Proceed to Step 2 for information on using the Source Address List Page 2 in the wizard.
   - To apply the DNS rule to requests originating from a list of DNS proxies that you have configured using the Source Address Lists function, click **Predefined source address list**, and then click **Next**. Proceed to Step 3 for information on using the Source Address List Page 3 in the wizard.

2. If you chose the Manually-entered Source Address List option in the Source Address List section of the wizard, use the Source Address List Page 2 of the wizard to create your Source Address List. Configuring the source address list by using the wizard makes it available for use by other DNS rules.
   - Enter a name for your Source Address List in the List Name field.
   - (Optional) Click the **List Owner** drop-down list and choose a GSS owner name.
   - In the space provided, enter one or more source classless interdomain routing (CIDR)-format IP addresses that make up the list. You can enter individual IP addresses or address blocks. If you want to enter multiple IP addresses, separate the addresses using semicolons. For example, enter:
     - 192.168.1.110/32; 192.168.10.0/24; 192.161.0.0/16
     - or
     - 2001:DB8::/64; 2001:DB8::1/128
   - Click **Next** to proceed to the Domain List detail page of the DNS Rule Wizard. See the “Specifying a Domain List in the DNS Rule Wizard” section for information.

3. If you chose the Predefined Source Address List option in the Source Address List section of the wizard, use the Source Address List Page 3 of the wizard to select an existing source address list.
   - Click the name of the source address list in the list to highlight it.
   - Click **Next** to select the source address list and proceed to the Domain List detail page of the DNS Rule Wizard. See the “Specifying a Domain List in the DNS Rule Wizard” section for information.

### Specifying a Domain List in the DNS Rule Wizard

The Domain List section of the DNS Rule Wizard allows you to specify the domains that users will request. Each GSS can support up to 2000 total domains. If using a KAL-AP type answer, the GSS can support up to 1024 domains managed by any single server load-balancing device such as a Cisco Content Services Switch (CSS) or Content Switching Module (CSM).
To specify a domain list in the DNS Rule Wizard, perform the following steps:

1. **Apply the DNS rule to requests for a hosted domain that you want to configure by clicking Manually-entered domain list**, and then clicking Next. Proceed to Step 3 for information on using the Domain List Page 2 in the wizard.

   or

2. **Apply the DNS Rule to requests for a domain from a list of hosted domains previously configured using the Domain Lists function by clicking Predefined domain list**, and then clicking Next. Proceed to Step 4 for information on using the Domain List Page 3 in the wizard.

3. If you chose the Manually-entered Domain List option in the Domain List section of the wizard, use the Domain List Page 2 of the wizard to manually configure the requested domains names. Configuring the domain list using the DNS Rule Wizard makes it available for use by other DNS rules.

   a. Enter a name for your Domain List in the List Name field.

   b. (Optional) Click the List Owner drop-down list and choose an owner name.

   c. In the space provided, enter the names of any hosted domains that you want to add to the domain 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.

      Hosted domains cannot exceed 128 characters. The following examples show domain names configured on the GSS:

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

      If entering multiple domain names, separate each name with a semicolon, for example, enter:

      www.cisco.com; support.cisco.com; cdn.cisco.com

      The GSS supports domain names that use wildcards. The GSS supports POSIX 1003.2-extended regular expressions when matching wildcards. Any request for a hosted domain that matches the pattern is directed accordingly.

      For example, assume that you have 20 or more possible domains, such as www1.cisco.com, www2.cisco.com, and so on. You can create a wildcard expression that covers all of those domains:

      .*\.cisco\.com

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

   d. When you complete entering the domain names, click Next to proceed to the Answer Group detail page of the DNS Rule Wizard. See the Configuring an Answer Group in the DNS Rule Wizard section for information.
4. If you chose the Predefined Domain List option, use Domain List Page 3 of the wizard to choose from a list of previously configured domains.
   a. Click the name of the domain list so that its name is highlighted.
   b. Click **Next** to choose the domain list and proceed to the Answer Group detail page of the DNS Rule Wizard. See the “Configuring an Answer Group in the DNS Rule Wizard” section for information.

### Configuring an Answer Group in the DNS Rule Wizard

The Answer Group section of the DNS Rule Wizard allows you to configure answers for a specific answer group type: VIP, NS, or CRA. Answers are a group of resources that the GSS considers for the response to the requesting client’s DNS proxy.

To configure an answer group in the DNS Rule Wizard, perform the following steps:

1. Have the DNS rule respond to the request for the hosted domain using resources (answers) that you want to configure by clicking **Enter addresses**, and then clicking **Next**. Proceed to Step 3 for information on using the Answer Group Page 2 in the wizard.

   or

2. Have the DNS rule respond to the request for the hosted domain using resources (answers) previously configured using the Answer Group function by clicking **Select an existing answer group**, and then clicking **Next**. Proceed to Step 4 for information on using the Answer Group Page 3 in the wizard.

3. If you chose the Enter Addresses option in the Answer Group section of the wizard, use Answer Group Page 2 in the wizard to create your answer group. Configuring the answer group using the DNS Rule Wizard makes it available for use by other DNS rules.
   a. Enter a name for your answer group in the Group Name field.
   b. (Optional) Choose an owner for the answer group by clicking the **Group Owner** drop-down list and selecting a GSS owner from the list.
   c. Select an answer group type by clicking one of the three option buttons. Once you select an answer group type, only answers of that type (VIP, NS, or CRA) can be added to the group:
      - VIP—Virtual IP (VIP) addresses associated with an SLB as such the Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, LocalDirector, web server, cache, or other geographically dispersed SLBs 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 requests back to a user’s D-proxy.
   d. Click **Next** to use the Answer Group Page 3 of the wizard to configure answers for your answer group. Proceed to Step 4.

4. Use Answer Group Page 3 of the DNS Rule Wizard to configure answers for the specified answer group type: VIP, NS, or CRA.

5. Perform one of the following actions:
   - If configuring a VIP-type answer group, perform the following steps to identify the VIPs that provide the answers that make up the answer group. Assign an order, load threshold, and weight to each answer in the answer group.
a. Enter the address of each VIP that belongs to the answer group in the IP Address fields provided.

b. Click the Location drop-down list and choose an optional Location.

c. If using the Weighted Round-Robin balance method, click the Weight drop-down list and assign a weight between 1 and 10 to each answer in the answer group.

d. If using the Ordered List balance method, assign an order to each VIP listed in the answer group using the Order field provided. The number that you assign represents the order of the answer in the list. Subsequent VIPs on the list will only be used if the preceding VIPs on the list are unavailable. 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.

e. If using a KAL-AP-type answer, assign a load threshold between 0 and 255 using the Load Threshold field. If the VIP answer reports a load above the specified threshold, the GSS will determine that the device is unavailable to handle further requests.

• If configuring a new name server-type answer group, perform the following steps to identify the name servers that provide the answers for the answer group:

a. Enter the address of each name server that belongs to the answer group to the IP Address fields provided.

b. For each name server IP address, choose an optional location by clicking the Location drop-down list.

c. If using the Weighted Round-Robin balance method, click the Weight drop-down list and assign a weight between 1 and 10 to each answer in the answer group. The weight is used to create 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 will receive 10 requests for every 1 directed to Answer B.

d. If using the Ordered List balance method with this answer group, assign an order to each name server listed in the answer group using the Order drop-down list provided. The number that you assign represents the order of the answer in the list. Subsequent name servers on the list will only be used if the preceding name servers on the list are unavailable. 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.

• If configuring a CRA-type answer group, perform the following steps to identify the CRAs that provide the answers that make up the answer group, and then assign a location for each answer in the answer group.

a. Enter the address of each CRA that belongs to the answer group in the IP Address fields provided.

b. For each CRA IP address, choose an optional location by clicking on the Location drop-down list.
c. Click Next to proceed to the Balance Method details page of the DNS Rule Wizard. See the “Choosing a Balance Method in the DNS Rule Wizard” section for information.

6. If you chose the Select an Existing Answer Group option, use Answer Group Page 4 in the wizard to choose from a series of previously configured answers.

   a. Click the name of the answer group in the list so that the name is highlighted.
   b. Click Next to choose the answer group and proceed to the Balance Method details page of the DNS Rule Wizard. See the “Choosing a Balance Method in the DNS Rule Wizard” section for information.

Choosing a Balance Method in the DNS Rule Wizard

The Balance Method page of the DNS Rule Wizard allows you to choose a balance method that specifies how a GSS answer should be chosen from the answer group to respond to a given DNS query. Your choice of balance methods is controlled by the type of answer group (name server, VIP, or CRA) that you choose.

Note

The DNS Rule Wizard supports the selection of a single balance clause. If necessary, you can modify the DNS rule and add additional balance clauses using the DNS Rule Builder (see the “Modifying DNS Rules” section).

To choose a balance method in the DNS Rule Wizard, perform the following steps:

1. If configuring a VIP or name server answer group to respond to requests, choose from the following balance methods for each of your DNS rule clauses:

   • 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.
     
     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.
   
   • 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. Least Loaded is available only for VIP-type answer groups that use a KAL-AP keepalive.
   
   • Ordered List—The GSS selects an answer based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding responses or answer 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.

   • Round Robin—The GSS cycles through the list of answers that are available as requests are received.
- 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.

2. If configuring a CRA answer group to respond to requests, the GSS automatically assigns Boomerang as the balance method. Enter a “last gasp” address in the Last Gasp field provided. This address serves as the answer in the event that no content routing agents reply to the request. When you specify a “last gasp” address, the GSS automatically performs the following:
   - Creates an answer for this address
   - Creates an answer group that contains the “last gasp” answer
   - Adds a second balance clause to the DNS rule with the suffix -GROUP and uses an ordered list as the balance method.

3. Click Next to proceed to the Summary page of the DNS Rule Wizard. An overview of your rule is provided that supplies information on the selected source address list, domain List, answer group, and balance method. See the Reviewing the Summary Page in the DNS Rule Wizard section for information.

**Reviewing the Summary Page in the DNS Rule Wizard**

The Summary page of the DNS Rule Wizard allows you to verify information about your DNS rule, including information on the selected source address list, domain list, answer group, and balance method.

To complete your DNS rule in the Summary page, perform the following steps:

1. Enter a name for your DNS Rule in the **Rule Name** field.

2. (Optional) Associate the rule with a GSS owner by choosing an owner name from the Rule Owner drop-down list.

3. Indicate the type of DNS queries that apply to this rule. Choose a query type from the Match DNS Query Type check box:
   - **All**—The DNS rule is applied to all DNS queries that originate from a host on the configured source address list. For any request other than an A and AAAA 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 then delivers the response to the requesting client D-proxy.
     
     When you choose All as the Match DNS Query Type, you must configure one balance clause to include a name server-type answer group.

   - **A record**—The DNS rule is applied only to answer address record (A-record) requests originating from a host on the configured source address list. For any request with an unsupported query types (for example, MX, PTR, or CNAME record) that match this DNS rule, those query types will be 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 in order for the requester to make a subsequent A-record query.

   - **AAAA record**—The DNS rule is applied only to answer address record (AAAA record) requests originating from a host on the configured source address list. For any request with unsupported query types (for example, MX, PTR, or CNAME record) that match this DNS rule, those query types are dropped and are not answered by the GSS. For an A record query with a configured host domain, the GSS returns a NODATA (No Answer, No Error) response in order for the requester to then make a subsequent A-record query.
**Building DNS Rules Using the DNS Rule Builder**

If you are familiar with the process of building a DNS rule and have previously configured your domain lists, answers, and answer groups, use the DNS Rule Builder to quickly assemble a DNS rule.

If you intend to use the DNS rule builder for more advanced GSS load-balancing applications such as DNS sticky or network proximity, see Chapter 9, Configuring DNS Sticky, or Chapter 10, Configuring Network Proximity, for the configuration procedures.

To create a DNS rule using the DNS Rule Builder, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab, and then click the **DNS Rules** navigation link. The DNS Rules list appears.

2. Click the **Open Rule Builder** icon. The DNS Rule Builder page opens in a separate window.

3. In the Rule Name field, enter a name for your new DNS Rule. Rule names cannot contain spaces.

4. From the Rule Owner drop-down list, choose a contact with whom the rule will be associated. The default Rule Owner is System.

5. From the Source Address List drop-down list, choose a 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.

6. From the Domain List drop-down list, choose a 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.

7. From the Match DNS Query Type check box, indicate what type of DNS queries applies to this rule:
   - **All**—The DNS rule is applied to all DNS queries that originate from a host on the configured source address list. For any request other than an A and AAAA 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.

     When you choose All as the Match DNS Query Type, you must configure one balance clause to include a name server-type answer group.
• A record—The DNS rule is applied only to answer address record (A-record or AAAA-record) requests that originate from a host on the configured source address list. For any request with unsupported query types (for example, MX, PTR, or CNAME records) that match this DNS rule, those query types will be 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 or AAAA-record query.

• AAAA record—The DNS rule is applied only to answer address record (AAAA record) requests originating from a host on the configured source address list. For any request with unsupported query types (for example, MX, PTR, or CNAME record) that match this DNS rule, those query types are dropped and are not answered by the GSS. For an A record query with a configured host domain, the GSS returns a NODATA (No Answer, No Error) response in order for the requester to then make a subsequent A-record query.

Note: In the DNS rule A and AAA, record types can be selected simultaneously.

The configured rule is applied to answer address record (A and AAAA record) requests originating from a host on the configured source address list. For any request with unsupported query types (for example, MX, PTR, or CNAME record) that match this DNS rule, those query types are dropped and are not answered by the GSS.

8. Disable sticky for the DNS rule by clicking None (default) as the Select Sticky Method option. This setting overrides the enabled state on the Global Sticky Configuration details page.

If you plan to configure DNS sticky in the DNS rule, see “Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups” in Chapter 9, Configuring DNS Sticky.

9. At the Balance Clause 1 heading, do the following:

• Choose the answer group component of your first answer group/balance method pairing from the drop-down list. This is the first effort the GSS uses to select an answer for the DNS query.

• Choose the balance method for the answer group from the drop-down list. Your choice of balance methods changes based on the type of answer group (VIP, name server, or CRA) that you selected.

10. If you chose a VIP or name server answer group to respond to requests, choose from the following balance methods for each of your DNS rule clauses:

Note: If you select a CRA-type answer group, the balance method is automatically set to Boomerang.

• 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.

  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.

• 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 balance method is available only for VIP-type answer groups that use a KAL-AP keepalive.
Ordered List—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. 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.

Round Robin—The GSS cycles through the list of answers that are available as requests are received.

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.

If you chose a VIP-type answer group, a series of fields appear below the active balance clause on the Create New DNS Rule window.

Configure the following VIP-type configuration information in the fields provided below the active balance clause:

- DNS TTL—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.
- Return Record Count—The number of address records (A-records) that you want the GSS to return for requests that match the DNS rule.
- Sticky Enable—Determines the DNS sticky for the balance clause when you click the Sticky Enable check box. This check box only appears when you enable sticky for the DNS rule, at the Select Sticky Method option. Note that 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.
- Region Sticky Enable—Determines the DNS region sticky for the balance clause when you click the Region Sticky Enable check box. This check box only appears when you enable sticky for the DNS rule, at the Select Sticky Method option. Note that 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 applies attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.
- Proximity Enable—If you plan to configure network proximity as part of the DNS rule balance clause, see the “Using the DNS Rule Builder to Add Proximity to a DNS Rule” section in Chapter 10, Configuring Network Proximity.
- Geodb Enable—The Geodb proximity for the balance clause. You can configure the GeoDB proximity only when the answers in the answer group are contained in locations that relate to a zone.
- Manual Reactivation—Determines whether the GSS reactivates the clause automatically when its state changes from unavailable to available or if you must manually reactivate the clause. Check the check box to enable the manual reactivation function.

A clause becomes unavailable for use by the GSS when all the answers in the answer group associated with it are either offline or overloaded. When at least one of the answers returns to an online state, the clause becomes available once again and the GSS, by default, begins using it. To manually control when the GSS reverts to using a clause that returns to an available state, you enable the manual reactivation function from the primary GSSM.
If you enable the manual reactivate function for a clause, you must also enable the global manual reactivate function for it to work (see the “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8).

- Status—Determines the operating state of the clause. Select one of the following options from the drop-down list:
  - Active—The DNS rule immediately begins processing requests.
  - Suspended—The DNS rule is listed on the DNS Rules list page but has a status of “suspended.” The DNS rule is not used to process any incoming DNS queries.
  
  For more information, see the “Suspending a Clause” and “Reactivating a Clause” sections.

12. If you chose a CRA-type answer group, a series of fields appear below the active balance clause on the DNS Rule Builder window.

  Configure the following configuration information in the fields provided below the active balance clause:

  - DNS TTL—The duration of time in (units) 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.
  - Fragment Size—The preferred size of the boomerang race response that is produced by a match to a DNS rule and sent to the requesting client.
  - Pad Size—The amount of extra data (in bytes) included with each CRA response packet and used to evaluate CRA bandwidth and latency when making load-balancing decisions.
  - IP TTL—The maximum number of network hops that should be utilized when returning a response to a CRA from a match on a DNS rule.
  - Secret—A text string, up to 64 characters, that is used to encrypt critical data sent between the GSS boomerang server and CRAs. This key must be the same for each configured CRA.
  - Max Prop. Delay—The maximum propagation delay, which is the maximum delay (in milliseconds) observed before the boomerang server component of the GSS forwards a DNS request to a CRA.
  - Server Delay—The maximum delay (in milliseconds) 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.
  - Manual Reactivation—Determines whether the GSS reactivates the clause automatically when its state changes from unavailable to available or if you must manually reactivate the clause. Check the check box to enable the manual reactivation function.

  A clause becomes unavailable for use by the GSS when all the answers in the answer group associated with it are either offline or overloaded. When at least one of the answers returns to an online state, the clause becomes available once again and the GSS, by default, begins using it. To manually control when the GSS reverts to using a clause that returns to an available state, you enable the manual reactivation function from the primary GSSM.

Note If you enable the manual reactivate function for a clause, you must also enable the global manual reactivate function for it to work (see the “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8).
Chapter 7      Building and Modifying DNS Rules

Modifying DNS Rules

You can use the DNS Rule Builder or the DNS Rule Wizard to modify a DNS rule.

Note If you have the manual reactivation function enabled for a clause and the GSS has the clause operationally suspended, modifying the clause will reactivate it.

To modify a DNS rule using the DNS Rule Builder, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab. The DNS Rules list appears.
2. Click the Modify DNS Rule Using Rule Builder Interface button located to the left of the DNS rule that you want to modify. The Modify DNS Rule details page opens in a separate window.
3. Make modifications as necessary to the DNS rule. See the “Building DNS Rules Using the DNS Rule Builder” section for details about using the DNS Rule Builder.
4. Click Save when you complete your modifications and return to the DNS Rules list page.

To modify a DNS rule using the DNS Rule Wizard, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab. The DNS Rules list appears.
2. Click the Modify DNS Rule Using Wizard button located to the left of the DNS rule that you want to modify. The Modify DNS Rule Wizard appears.
3. Make modifications as necessary to the DNS rule in the DNS Rule Wizard. See the “Building DNS Rules Using the Wizard” section for details about using the DNS Rule Wizard.
4. Click Finish when you complete your modifications and return to the DNS Rules list page.
Suspending a Clause

You can temporarily stop the GSS from using an active clause associated with a rule by performing the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab. The DNS Rules list page appears.
2. Click the **Modify DNS Rule Using Rule Builder Interface** icon located to the left of the DNS rule that you want to suspend. The DNS Rule Builder page appears in a separate browser window.
3. Choose **Suspended** from the Status drop-down list.
4. Click **Save** to save your DNS Rule. You return to the DNS Rules list page. The DNS rule clause is now suspended.

Reactivating a Clause

You can reactivate a clause that you suspended by performing the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab. The DNS Rules list page appears.
2. Click the **Modify DNS Rule Using Rule Builder Interface** icon located to the left of the DNS rule that you want to suspend. The DNS Rule Builder page appears in a separate browser window.
3. Choose **Active** from the Status drop-down list.
4. Click **Save** to save your DNS Rule. You return to the DNS Rules list page. The DNS rule clause is now active.

Reactivating Operationally Suspended Clauses

When you enable the manual reactivation function in a clause configuration and the clause becomes unavailable for use by the GSS, the primary GSSM operationally suspends the clause. The clause remains operationally suspended even when it returns to an available state and is ready for service. This enables you to manage when the GSSs on the GSS mesh revert to using all operationally suspended clauses.

Use the Manual Reactivation navigation link in the Resources tab to reactivate operationally suspended clause. For information, see “Managing Global Manual Reactivation of Answers and Clauses” section on page 2-8.

Suspending a DNS Rule

If you want to stop requests from being processed by a DNS rule on your GSS, use the Suspend icon to temporarily deactivate the rule. You can use the suspend feature to temporarily halt traffic to particular answers while those resources are receiving maintenance. Once you suspend a DNS rule, you must reactivate the rule before you can use it to process incoming DNS queries.

To suspend a DNS rule from the DNS Rule Builder, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab. The DNS Rules list page appears.
2. Click the **Modify DNS Rule Using Rule Builder Interface** icon located to the left of the DNS rule that you want to suspend. The DNS Rule Builder page appears in a separate browser window.
Reactivating a DNS Rule

To suspend a DNS rule from the DNS Rule Wizard, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab. The DNS Rules list page appears.
2. Click the Modify DNS Rule Using Wizard icon located to the left of the DNS rule that you want to suspend. The DNS Rule Wizard appears.
3. Click the Summary navigation link in the Wizard Contents table of contents. The Summary page appears.
4. From the Rule Status drop down list, choose the Suspended operating status for the DNS rule.
5. Click Finish to confirm your decision and return to the DNS Rule list page. The status of the DNS rule appears as “Suspended.”

To reactivate operation of a suspended DNS rule from the DNS Rule Builder, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab. The DNS Rules list page appears.
2. Click the Modify DNS Rule Using Rule Builder Interface icon located to the left of the DNS rule that you want to activate. All suspended DNS rules have a status of “Suspended” in the list. The DNS Rule Builder window appears.
3. Click the Activate icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to activate the DNS rule.
4. Click OK to confirm your decision. You return to the DNS Rule list page. The status of the DNS rule appears as “Active.”
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 can simplify the process to suspend or activate all rules related to a particular group or department within your organization (for example, HR or Sales) without requiring to individually edit each rule that serves that owner.

To suspend or reactivate DNS rules belonging to an owner, perform the following steps:

1. From the primary GSSM GUI, click Resources tab.
2. Click the Owners navigation link. The Owners list page appears.
3. Click the Modify Owner icon located to the left of the owner responsible for the DNS rules that you want to suspend or reactivate. The Modifying Owner details page appears.
4. Perform one of the following:
   - To suspend all DNS rules associated with this owner, click the Suspend All DNS Rules for This Owner icon in the upper-right corner of the details page.
   - To reactivate all suspended DNS rules associated with this owner, click the Activate All DNS Rules for This Owner icon in the upper-right corner of the details page.
5. Click OK to confirm your decision to suspend or activate the answers. You return to the Owner list page.

Deleting a DNS Rule

Use the Delete icon 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. From the primary GSSM GUI, click the DNS Rules tab. The DNS Rules list page appears.
2. Click the Modify DNS Rule using rule builder interface icon located to the left of the DNS rule that you want to delete. The DNS Rule Builder window appears.
3. Click the Delete icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the DNS rule.
4. Click OK to confirm your decision. You return to the DNS Rule list page.
Configuring DNS Rule Filters

As your GSS network grows, so will your collection of DNS rules for handling traffic to and from your network. In time, it may become difficult to locate the rules that you need. For that reason, the primary GSSM GUI provides filters that you can apply to your DNS rules to view only those rules that have the properties in which you are interested. For example, you can create a filter that will limit your view of the DNS rules to include only those rules that involve a certain source address list or domain list, use a certain balance method, are owned by a particular user, or have a status of “active.”

To configure a DNS rule filter, perform the following steps:

1. From the primary GSSM GUI, click the DNS Rules tab.
2. Click the Filter DNS Rule List icon. The Configure DNS Rule List Filter details page appears.
3. Filter your list by any of the properties displayed on the Filter List page by entering a complete or partial (wildcard) value into the fields provided. The GUI divides the Filter List page by Source Address List Filter Parameters, Domain List Filter Parameters, Balance Clause Filter Parameters, and DNS Rule Filter Parameters. The GSS supports filtering combinations in the properties of all four sections of the details page.

Table 7-1 lists the parameters that you can use to filter your DNS rules list, along with explanations and sample entries for each parameter.

<table>
<thead>
<tr>
<th>Table 7-1 DNS Rules Filter Parameters</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Selection Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Address List Filter Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to a source address list associated with the DNS rule</td>
<td>VIP1, VIP*, NameServerList</td>
</tr>
<tr>
<td>IP Address Block</td>
<td>IP address or address block assigned to a source address list associated with the DNS rule</td>
<td>192.168.110.100, 2001:DB8::1, 192.168.<em>, 2001:DB8::</em></td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the owner assigned to the source address list associated with the DNS rule</td>
<td>Any, System, Education</td>
</tr>
</tbody>
</table>

| **Domain List Filter Parameters** | | |
| Name | Name assigned to a domain list associated with the DNS rule | CiscoSystems, Cisco* |
| Domain | Domain included on the domain list associated with the DNS rule | www.cisco.com, support.cisco.com, www.* |
| Owner | Name of the owner assigned to the domain list associated with the DNS rule | Any, System, Sales |
### Configuring DNS Rule Filters

<table>
<thead>
<tr>
<th><strong>IP Address Block</strong></th>
<th>IP address or address block assigned to a source address list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.110.100</td>
</tr>
<tr>
<td></td>
<td>2001:DB8::1</td>
</tr>
<tr>
<td></td>
<td>192.168.*</td>
</tr>
<tr>
<td></td>
<td>2001:DB8::*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Owner</strong></th>
<th>Name of the owner assigned to the source address list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Domain List Filter Parameters</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name assigned to a domain list associated with the DNS rule</td>
</tr>
<tr>
<td></td>
<td>CiscoSystems</td>
</tr>
<tr>
<td></td>
<td>Cisco*</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Domain included on the domain list associated with the DNS rule</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
<tr>
<td></td>
<td>support.cisco.com</td>
</tr>
<tr>
<td></td>
<td><a href="http://www">www</a>.*</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Name of the owner assigned to the domain list associated with the DNS rule</td>
</tr>
<tr>
<td></td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Sales</td>
</tr>
</tbody>
</table>

---
### Configuring DNS Rule Filters

<table>
<thead>
<tr>
<th>IP Address Block</th>
<th>IP address or address block assigned to a source address list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.110.100</td>
</tr>
<tr>
<td></td>
<td>2001:DB8::1</td>
</tr>
<tr>
<td></td>
<td>192.168.*</td>
</tr>
<tr>
<td></td>
<td>2001:DB8::*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Owner</th>
<th>Name of the owner assigned to the source address list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
</tbody>
</table>

### Domain List Filter Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Name assigned to a domain list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CiscoSystems</td>
</tr>
<tr>
<td></td>
<td>Cisco*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Domain included on the domain list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
<tr>
<td></td>
<td>support.cisco.com</td>
</tr>
<tr>
<td></td>
<td><a href="http://www">www</a>.*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Owner</th>
<th>Name of the owner assigned to the domain list associated with the DNS rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Sales</td>
</tr>
</tbody>
</table>


### Table 7-1  DNS Rules Filter Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Selection Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance Method</td>
<td>Type of balance method (such as boomerang and ordered list) associated with the DNS rule</td>
<td>Boomerang</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hashed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Least-Loaded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Order List</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Round-Robin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Weighted Round-Robin</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the DNS rule</td>
<td>Cisco_Rule</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the owner assigned to the DNS rule</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sales</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the DNS rule, either active or suspended</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suspended</td>
</tr>
</tbody>
</table>
4. Click **Submit** to confirm your decision and return to the DNS Rule list page. The displayed DNS rules are those DNS rules that match your search criteria. If no DNS Rule parameters match the parameters that you used to filter the list, a message appears:

```
No DNS rules match the filter specification.
```

## Removing DNS Rule Filters

You can use the Show All DNS Rules icon on the DNS Rules list page to remove any filters applied to DNS rules. The Show All DNS Rules icon removes all filters and displays a complete list of DNS rules on your GSS network.

To remove DNS rule filters, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab. The DNS Rules list page appears.
2. Click the **Show All DNS Rules** icon. The DNS Rule Filter list page refreshes, displaying all configured DNS rules.

## 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  192.168.1.1
; Cisco GSS London
  gss2 IN A  192.168.3.6

When you review this zone file, note that there are any number of possible GSS deployments you can use; some deployments may suit your needs and your network better than the listed example. For instance, instead of having all subdomains shared by all GSS devices, you may want to allocate specific subdomains to specific GSSs.

Where To Go Next

Chapter 8, “Configuring and Monitoring the GeoDB”, describes how to implement GeoIP database-based proximity computation mechanism in GSS.
CHAPTER 8

Configuring and Monitoring the GeoDB

This chapter describes how to implement the GeoIP database (GeoDB) proximity computation mechanism in GSS. From the latitudinal and longitudinal information in the GeoDB, GSS decides the proximity, based on the geographical distance from the client D-proxy instead of the round-trip time (RTT) value. Once you determine the latitude and longitude of the client’s D-proxy and a resource in the data center, the GSS can calculate the distance. During the proximity calculation, the GSS uses these distances instead of RTT values to determine the IP address of the resource nearest to the D-proxy.

To enhance the various GSS features with GeoIP-awareness, you can add support for the GeoDB in locations. The process of updating the GeoDB does not impact GSS operations. All user-defined database entries are preserved during a database upgrade.

To enable the GeoDB feature, a valid license should be installed and the GeoIP database should be imported into GSS. If you want to enable the GeoDB license package on a particular GSS, you must purchase a GeoDB license from Cisco in order to receive a Product Authorization Key (PAK) number. For more information on obtaining and installing a GeoDB license, see the Global Site Selector Administration Guide. After importing, if static entries are present, the distance gets computed based on the latitude and longitude mentioned for the static entries.

Before you add or modify the regions or states, you must import the GeoIP database file. To import the GeoIP database file, see Where To Go Next.

The state names and country codes are getting stored in the gslb configuration of the GSS. When you do gss disable, the country name and state codes that are needed to create regions are stored as a gslb configuration is removed. To populate you must re-import the GeoDB file. It is recommended that you import the GeoDB file again for the proper functionality. The show geodb output command displays the status of the GeoDB tables that are available in the cache memory, while the codes reside in the gslb configuration.

This chapter contains the following major sections:

- Downloading GeoIP Database
- Monitoring GeoIP Database Download and Install Status
- Setting Up the Global GeoDB Configuration
- Managing the GeoDB Static Entries
- Monitoring GeoDB Statistics
- Where To Go Next
Downloading GeoIP Database

This section describes how to download the GeoIP database file using the Download GeoIP database navigation link in the GUI.

Also, if you want to download the GeoIP database file manually, see the Managing GeoDB Operations section in the Configuring and Monitoring the GeoDB chapter at the following URL on Cisco.com:

To download the GeoIP database file, perform the following steps:

1. From the primary GSSM GUI, click the GeoDB tab.
2. Click Database > Download GeoIP Database navigation link.
   The Maxmind Licence Page appears displaying the license information.
3. Proceed to GeoIP Database Download page by clicking I Agree button.
   The GeoIP Database Download and Install page appears.
4. If you do not agree with the licensing terms and conditions, click I Decline. You will be redirected to the GeoIP main page.
5. Using GeoIP database download page you can perform the following tasks:
   – Install—Installs the GeoIP database file that is previously downloaded.
   – Download and Install—Downloads and Installs the GeoIP database file.
6. Enter the user name, in the Maxmind’s User Name field.
7. Enter the Password, in the Maxmind’s password field.

Note For the maxmind user name and password, refer to the e-delivery letter of your GeoIP database license. For further assistance, contact your Cisco account representative or send an e-mail message to ask-gss@cisco.com.

Note If you have direct access to the Internet connectivity, proceed to Step 13 to download the database file from Maxmind. If you have to enable proxy support for the Internet connectivity, proceed to Step 8.

8. To enable the proxy support, check the Enable the Proxy support for downloading the GeoIP Database check box.
9. Enter the proxy server name or the IP address in the Proxy Server’s Name or IP Address field. For example, proxy-sjc 00.example.com or 192.168.1.1.
10. Enter the proxy server’s port number in the Proxy Server’s Port number field. The default proxy port is 1080.

Note • If your proxy server does not have a user name and password, proceed to Step 13.
The proxy server, port, user name, and password fields are enabled only if you enable the proxy support.

11. Enter the proxy server’s user name in the Proxy Server’s User Name field.
12. Enter the proxy server’s password in the Proxy Server’s Password field.
13. To ensure that you are downloading the latest GeoIP database file available in Maxmind website, check the Download latest GeoIP database check box and click icon.

   The File URL of the GeoIP Database field gets populated with the latest path where the database file is stored. For example, 

   Note that the date along with ‘v’ followed by numbers represents the version of the database file. For example, v001(2011-09-27) where v001 denotes the version and (2011-09-27) denotes the date.

   A dialog box appears and indicates that the installed or new version (if any) of the Geo IP database file.

14. Click Submit to start the GeoIP database download or Install or to download and Install together. After clicking Submit button go to GeoIP Database Status page to check the status of your operation for complete GSS mesh.
15. If you want to download a specific or previous version of the database file, edit the path with the version number, and then click Submit.

   For example, http://geolite.maxmind.com/download/sec/cisco_geodb_2011-08-28_v001.tar.gz

   Note If there is no previously downloaded GeoIP database file, and if you check the Install radio button, the GSS prompts you to download the file with the following message: No Downloaded file, Kindly download the file first to install it.

16. Click the Install radio button to install the database file, if you have a previously downloaded copy of the GeoIP database file.

   The GUI displays the following message:
   The latest downloaded file cisco_geodb_2011-09-27_v001.tar.gz will be installed.

17. Check the Clear Cache Entries while installing GeoIP Database check box to remove the cached look up result. By default, the check box is selected.
18. To cancel the GeoIP database file download, click CancelDownload.

### Monitoring GeoIP Database Download and Install Status

The GeoIP database download and install status page displays the following columns: the name of the Global Site Selector, the download status, the last downloaded version, the installation status and the last installed version.

To monitor the GeoIP database download and install status, perform the following steps:

1. From the primary GSSM GUI, click the GeoDB tab.
2. Click the GeoIP Database Status navigation link.

   The GeoIP database and install status page appears.
You can view the list of GSS names and the corresponding download status, the downloaded version, the install status, and the installed version in the respective columns. The four download status messages that can be seen in the status columns are as follows:

- In Progress—GeoIP database file download is in progress.
- Completed—GeoIP database file download is completed.
- md5checksum Failed—The downloaded tar file is corrupted.

The install status messages that can be seen in the status column are as follows:

- Failed-Md5Checksum—The downloaded tar file is corrupted.
- Failed-BadTarFile—The downloaded tar file is corrupted.
- Failed-DecryptionFailed—The downloaded file fails to decrypt.
- Failed-File not present—The GeoIP database file is not present in the GSS.
- Failed-Geodb license not installed—If you have not enabled the GeoIP database license, the database file gets downloaded on to the GSS, but will not be installed. The install status reads as “License Not Enabled.”
- Not Done—The GeoIP database file is not imported.
- Completed—The import is completed.
- Importing—The GeoIP database file importing is in progress.

**Note**
- If you have initiated the database file download, the database files are downloaded in the Primary GSS first, and then the database file is fetched to the other GSS’s in the network from the primary GSS.
- When the download fails in one or more GSS’s in the mesh, a message appears in the Download and Install Status Page. The message reads as “To Restart Download In All Failed GSS Click Here”, which provides a quick link for re-initiating the download on the failed GSS’s.
- If you have not enabled the GeoIP database license, the database file gets downloaded on to the GSS, but will not be installed. The install status reads as “License Not Enabled.”

### Setting Up the Global GeoDB Configuration

To set up the global GeoDB configuration settings, perform the following steps:

1. From the primary GSSM GUI, click the **GeoDB** tab.
2. Click the **Configuration** navigation link. The global GeoDB configuration page appears.
3. From the global GeoDB configuration page, do the following:
   a. Click one of the following radio buttons to set the GeoDB operating state:
      - **Disabled**—Disables the GeoDB feature.
      - **Enabled**—Enables the GeoDB feature. This is the default setting.
   b. In the Mask field, enter a global GeoIP static entry mask that the GSS uses to uniformly group contiguous addresses. You can enter the 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).
Managing the GeoDB Static Entries

This section shows how to manage the GeoDB static entries and contains the following topics:

- Adding a New GeoDB Static Entry
- Viewing GeoDB Static Entries

Adding a New GeoDB Static Entry

To create a new static entry in the GeoDB, perform the following steps:

1. From the primary GSSM GUI, click the GeoDB tab.
2. Click the Database navigation link. The global GeoDB configuration page appears.
3. From the Add Static Entries page, do the following:
   a. In the Start IP Address field, enter the start of the IP address range.
   b. In the End IP Address field, enter the end of the IP address range.
   c. From the Country drop-down list, choose the appropriate country.
   d. From the State drop-down list, choose the appropriate country.
   e. In the Latitude field, enter the latitude of the location where the IP address range is located.
   f. In the Longitude field, enter the longitude of the location where the IP address range is located.
4. Click the Submit button to save your changes.

Viewing GeoDB Static Entries

To view the number of Static Entries, perform the following steps:

1. From the primary GSSM GUI, click the GeoDB tab.
2. Click the Database navigation link and then click Show Static Entries. The show static entries list page appears displaying the following information:
   - **Start IP Address**—Start of an IP range.
   - **End IP Address**—End of an IP range.
   - **Latitude**—Latitude of the geographical location.
   - **Longitude**—Longitude of the geographical location.
   - **Country Code**—Country code that resides in the GeoDB configuration.
   - **State Name**—Name of the state that you have associated with a specific country.

### Monitoring GeoDB Statistics

This section contains the following topics:
- Monitoring GeoDB Rule Hit Stats
- Monitoring GeoDB Database Stats
- Monitoring GeoDB Lookup Stats

### Monitoring GeoDB Rule Hit Stats

The GeoDB rule hit stats list page displays the GeoDB rule hit statistics for each rule that has the GeoDB option enabled.

To view the number of GeoDB rule hit statistics, perform the following steps:
1. From the primary GSSM GUI, click the GeoDB tab.
2. Click the Statistics navigation link and then click GeoDB Rule Hit Stats. The GeoDB rule hit stats list page appears displaying the following information:
   - **Name**—Name assigned to the GeoDB rule using the primary GSSM.
   - **Owner**—GSS owner to which the GeoDB rule has been assigned.
   - **non.gss.com**—Name of the GSSM or GSS.

   **Note** Data may be delayed up to 300 seconds.

### Monitoring GeoDB Database Stats

The GeoDB database stats list page displays the status of the GeoDB engine, the number of entries in the cached GeoDB, the last cleanup time, and the number of cleanups.

To view the GeoDB Database Stats, perform the following steps:
1. From the primary GSSM GUI, click the GeoDB tab.
2. Click the Statistics navigation link and then click GeoDB Database Stats. The GeoDB database stats list page appears displaying the following information:
   - **Global Site Selector**—Name of the GSS or GSSM device.
Chapter 8 Configuring and Monitoring the GeoDB

Where To Go Next

- **Status**—Online status of each GSS 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.

**Note**
Data may be delayed up to 300 seconds.

**Monitoring GeoDB Lookup Stats**

The GeoDB lookup stats list page displays the number of lookup requests, the current lookup rate, the peak lookup rate, the number of DB entries found, the number of partial data, DB full dropped requests, and the last DB full timestamp.

To view the number of GeoDB Lookup Stats, perform the following steps:

1. From the primary GSSM GUI, click the **GeoDB** tab.
2. Click the **Statistics** navigation link and then click on **GeoDB Lookup Stats**. The GeoDB lookup stats list page appears displaying the following information:
   - **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 the GSS was unable to locate a proximate answer from the proximity database.
   - **Partial Data**—Number of times 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.

**Note**
Data may be delayed up to 300 seconds.

**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 9, 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 10, Configuring Network Proximity, for details.
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 locally and also globally between GSS peers in the network.

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 GUI
- Configuring Sticky Using the GSS 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 device. In addition, the primary GSSM GUI displays sticky statistics for the GSS network. See Chapter 11, Monitoring GSS Global Server Load-Balancing Operation, 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 or AAAA-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, which can disrupt 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 through the configuration of 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. The resource responds
as follows:

- If the resource is available (online state), the GSS uses this answer for the DNS response sent back
to the D-proxy.
- If the resource is 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.
- If the resource is 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 IPv4 address can 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 D-proxy IPv6
address can also be some form of an IPv6 Address if the global prefix length is set to a value other than
the default of 128.
Chapter 9      Configuring DNS Sticky

DNS Sticky Overview

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 make up each sticky database key that the GSS uses for the lookup, storage, and persistence of stickiness for DNS responses.

The sticky database (SDB) can store IPv6 D-proxy addresses, sticky answers that are returned for AAAA queries, Hit count for AAAA query answers, and IPv6 address entries in the sticky group configuration. The prefix length configuration in the global sticky property configuration supports to group all the matching IPv6 D-proxy addresses into the same sticky database (SDB). The SDB operations such as SDB look up, SDB delete can use IPv6 D-proxy and IPv6 answers.

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 respectively based on a user-specified global sticky inactivity timeout value. The sticky inactivity timeout value identifies the time period that an answer (A or AAAA) 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 again requesting the answer, the GSS identifies the answer (A or AAAA) 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 looks in 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 communicates updates to its remote GSS peers when any of the following situations 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 purging an answer from the sticky database due to reaching the normal sticky inactivity timeout or a sticky database overflow. It is expected that each GSS in the mesh performs 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.
Chapter 9 Configuring DNS Sticky

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 the GSS devices communicate their updates to each peer, the recipient detects a conflict. Conflicts are resolved in the peer network by each GSS keeping the record 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 if you do the following:

- Configure sticky DNS rules for one domain only. Avoid using the By Domain List selection for the sticky method unless absolutely necessary.
- Avoid using domain wildcards. Wildcard domains pose the same issue as domain lists.
- Set the DNS TTL value of each sticky balance clause to a higher value to allow the sticky database to synchronize answers before the client D-proxy attempts to re-resolve the answer. Avoid using low DNS TTL values in a sticky balance clause.

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 the clock of a GSS device is out of synchronization with the other GSS peers (greater than a 3 minute difference), 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 was made on the primary GSSM GUI 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 version of GSS software and has the same global subnet mask and prefix-length values.
- Sticky mesh communication occurs only over an IPv4 interface for the global sticky configuration.
- For the global sticky to function all GSS’s must run the same software version of GSS software. Mixed mode (combination of different software versions) should not be used as the SDB format is changed in GSS software version 41(0).

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 CLI command to restart the GSS software on the local GSS node.
- Enter the sticky stop and sticky start CLI command sequence on the local GSS node.
- Enter the reload CLI command to perform a cold restart of local GSS node.
Choose the **Global** state in the Global Sticky Configuration details page of the primary GSSM GUI from either the Disabled or Local state.

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 generates a burst of network traffic. In this case, you direct network traffic to a different peer other than the GSS identified as being the closest (with the shortest round-trip time).

When you identify a favored peer, upon reentry into the mesh, the local GSS node always attempts to first synchronize its sticky database entries with the favored GSS peer. If the GSS 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.

## DNS Sticky Quick Start Guide

Table 9-1 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 GUI page or the GSS CLI command required to complete the task. For the procedures to configure the GSS for DNS sticky, see the sections following the table.

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> 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.</td>
</tr>
<tr>
<td>For example, enter:</td>
</tr>
<tr>
<td>gss1.example.com&gt; <strong>enable</strong></td>
</tr>
<tr>
<td>gss1.example.com# <strong>config</strong></td>
</tr>
<tr>
<td>gss1.example.com(config)# <strong>ntp-server 192.168.1.1</strong></td>
</tr>
<tr>
<td>gss1.example.com(config)# <strong>ntp enable</strong></td>
</tr>
<tr>
<td><strong>2.</strong> Log in to the primary GSSM GUI.</td>
</tr>
<tr>
<td><strong>3.</strong> Click the Traffic Mgmt tab, and then click the Sticky navigation link to access the Global Sticky Configuration details page.</td>
</tr>
<tr>
<td><strong>4.</strong> At the State option, click one of the option buttons to enable DNS sticky for the GSS network:</td>
</tr>
<tr>
<td>• <strong>Local</strong>—Enables DNS sticky for each active GSS device on a local level only.</td>
</tr>
<tr>
<td>• <strong>Global</strong>—Enables DNS sticky across the entire GSS network. All local sticky features are in operation. In addition, all GSS peers in the network share sticky database information.</td>
</tr>
</tbody>
</table>
5. Modify one or more of the DNS sticky configuration default settings in the Global Sticky Configuration details page by performing the following steps:
   a. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses. Use this parameter to increase the number of D-proxies supported in the sticky database by grouping multiple D-proxies into a single database entry. 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).
   b. In the Entry Inactivity Timeout field, enter the maximum time interval, in minutes, for which an unused entry (answer) remains valid in the sticky database. This entry is the global default for the GSS. However, you can modify the inactivity timeout value for each DNS rule. 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 again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database.
   c. In the Prefix Length field, enter a global prefix length that the GSS uses to uniformly group contiguous IPv6 D-proxy addresses as an attempt to increase the number of clients that the sticky database can support. This prefix-length is applied to the client source IP address before accessing the sticky database. Enter the preferred prefix length. The range of the prefix length is from 1 to 128. The default prefix length is 128.

6. Configure inter-GSS global sticky mesh settings in the Global Sticky Configuration details page by performing the following steps:
   a. At the Mesh Encryption option, enable or disable the encryption of data transmitted by GSS devices in the mesh. The GSS support encryption of all inter-GSS communications to maintain the integrity of the sticky database information transferred among the mesh peers.
   b. To authenticate communication between GSS devices in the mesh to prevent unauthorized device access, enter a secret string in the Encryption String field. The secret string provides a key for authentication between GSS devices as well as for encryption (if enabled).
   c. If you want a local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, in the Favored Peers section identify a favored peer for each local GSS node in the mesh.

7. Click the Submit button to save your DNS sticky configuration changes.

8. Access the DNS Rule Builder by performing the following steps:
   a. Click the DNS Rules tab.
   b. Click the DNS Rules navigation link. The DNS Rules list appears.
   c. Click either the Open Rule Builder icon (if this DNS rule is new) or click the Modify DNS Rule Using Rule Builder Interface icon (if this rule already exists) to access the DNS Rule Builder.

Note The DNS sticky global server load-balancing application is configurable only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable sticky in a DNS rule.
Chapter 9  Configuring DNS Sticky

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 for a GSS to communicate with the other GSS devices in the peer mesh. If the clock of a GSS device 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 server(s) for each GSS device that operates in the global mesh before you enable DNS sticky for those devices from the primary GSSM GUI. 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:

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

```
gssm1.example.com(config)# ntp-server
```

```
gssm1.example.com(config-ntp)# ntp-server 10.0.0.1
```

```
gssm1.example.com(config-ntp)# ntp-server 10.0.0.2
```

Table 9-1  DNS Sticky Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Enable DNS sticky in a DNS rule using the DNS Rule Builder. Define the following DNS rule configuration information as follows:</td>
</tr>
<tr>
<td>a. At the Select Sticky Method option, choose one of the following sticky selections:</td>
</tr>
<tr>
<td>- By Domain—Enables DNS stickiness on a matching hosted domain.</td>
</tr>
<tr>
<td>- By Domain List—Enables DNS stickiness on a matching hosted domain list.</td>
</tr>
<tr>
<td>b. If you want to override the global Entry Inactivity Timeout value for this DNS rule, in the Inactivity Timeout field, enter the maximum time interval that can pass without the sticky database receiving a lookup request for an entry before the GSS removes the entry.</td>
</tr>
<tr>
<td>c. For each balance clause that you want to perform DNS sticky load balancing, click the Sticky Enable checkbox.</td>
</tr>
</tbody>
</table>

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.

10. (Optional) Group multiple D-proxy IP addresses as a single entry in the sticky database by logging on to the CLI of the primary GSSM, enabling privileged EXEC mode, accessing the global server load-balancing configuration mode, and using the sticky group command.

```
gssm1.example.com> enable
gssm1.example.com(config)# sticky group StickyGroup1 ip 192.168.3.0 netmask 255.255.255.0
```

```
gssm1.example.com(config)# sticky group StickyGroup1 ip 2001:1:1:1:: netmask 112
```

```
gssm1.example.com(config)# sticky group StickyGroup1
```
**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, 192.168.1.1) 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 to enable the NTP service:

```
gss1.example.com> enable
gss1.example.com# config
s1.example.com(config)# ntp-server 192.168.1.1 192.168.1.2
s1.example.com(config)# ntp enable
```

## Configuring Sticky Using the Primary GSSM GUI

This section describes how to configure GSS devices for DNS sticky operation from the primary GSSM GUI and how to add stickiness to a DNS rule using the DNS Rule Builder. It contains the following topics:

- Configuring DNS Sticky
- Configuring the Global Sticky Mesh
- Enabling Sticky in a DNS Rule

### 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 GUI, choose **Global** or **Local** for the State option in the Global Sticky Configuration details page.
- A sticky method option (domain or domain list) is selected. In the GUI, use the DNS Rule Builder and choose **By Domain** or **By Domain List** for the Select Sticky Method option in the Create New DNS Rule window.
- Sticky is enabled within a balance clause for the DNS rule. In the GUI, use the DNS Rule Builder and click the **Sticky Enable** checkbox.

You enable sticky and configure the DNS sticky settings for the GSS network through the Global Sticky Configuration details page of the Traffic Mgmt tab. Changing a DNS sticky setting and applying that change is immediate and modifies the default values of the DNS sticky settings used by the DNS Rule Builder.

To configure DNS sticky from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Sticky** navigation link. The Global Sticky Configuration details page appears.

3. At the State option, click one of the following option buttons to enable or disable sticky for the GSS network:
   - **Disabled**—Disables DNS sticky across the GSS network. When you disable sticky, the GSS answers DNS requests for all domains and clients, subject to DNS rule matching, without accessing the sticky database or sharing sticky database information between peers in the network.
   - **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.
   - **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.

4. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of clients that the sticky database can support. Enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in /n notation. The range of prefix-length is from 1 - 128 (for example, /24).

   This mask is applied to the client source IP address before accessing the sticky database. 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), if the incoming D-proxy address does not match any of the entries in a defined DNS sticky group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

5. In the Prefix Length field, enter a global prefix length that the GSS uses to uniformly group contiguous IPv6 D-proxy addresses as an attempt to increase the number of clients that the sticky database can support. This prefix length is applied to the client source IP address before accessing the sticky database. Enter the preferred prefix length. The range of the prefix length is from 1 to 128. The default prefix length is 128.

   When you define a DNS sticky group for incoming IPv6 D-proxy addresses, if the incoming IPv6 D-proxy address does not match any of the entries in a defined DNS sticky group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

6. In the Entry Inactivity Timeout field, enter the maximum time period that an unused answer remains valid in the sticky database. Enter a value from 15 to 10080 minutes (168 hours), specified in 5 minute intervals (15, 20, 25, 30, up to 10080).

   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 inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. The default value is 60 minutes.

   The Inactivity Timeout value can also be set individually for each DNS rule. When you set an Inactivity Timeout value for a DNS rule, that value overrides the global Entry Inactivity Timeout value.
7. Click the **Submit** button to save your DNS sticky configuration changes.

To configure inter-GSS operation in the global sticky mesh through the Global Sticky Configuration details page, see the “Configuring the Global Sticky Mesh” section.

## Configuring the Global Sticky Mesh

The GSS includes a set of parameters to configure inter-GSS global sticky mesh operation. You configure mesh operation through the Global Sticky Configuration details page of the Traffic Mgmt tab. To configure the inter-GSS device mesh operation from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.

2. Click the **Sticky** navigation link. The Global Sticky Configuration details page appears.

3. Ensure that you set the State option to **Global**.

4. At the Mesh Encryption option, enable or disable the encryption of data transmitted by GSS devices in the mesh. The GSS supports encryption of all inter-GSS communications throughout the mesh to maintain the integrity of the sticky database information transferred among the GSS peers as follows:
   - Disabled—Disables the encryption of data transferred between GSS peers in the mesh. The application data is transmitted in clear text.
   - Enabled—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.

5. Authenticate communication between GSS peers in the mesh to prevent unauthorized device access by entering a secret string in the Encryption String field. Enter an unquoted text string with a maximum of 32 characters and no spaces.

   The secret string provides a key for authentication between GSS peers 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. You globally configure the shared secret on the primary GSSM GUI, which is used by all mesh peers.

6. If you want a local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, in the Favored Peers section, identify a favored peer for each local GSS node in the mesh.

   By identifying a favored GSS peer, you can also reduce network issues with peer synchronization, which typically generates a burst of network traffic. In this case, you can direct network traffic to a different peer other than the GSS identified as being the closest (with the shortest round-trip time). The Favored Peers section of the page presents an array of all local GSS nodes in the mesh along with a drop-down list of the remote peers.

   A GSS joins the mesh upon one of the following:
   - A reload.
   - A power up.
- When you enter a `gss stop` and `gss start` CLI command sequence.
- When you enter a `gss reload` CLI command.
- When you enter a `sticky stop` and `sticky start` CLI command sequence.
- When you choose the `Global` state in the Global Sticky Configuration details page from either the Disabled or Local state.

Upon reentry into the mesh, the local GSS node first attempts to synchronize its sticky database entries with the 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 node gss_1 to gss_3 as its favored peer, and direct local node gss_2 to gss_4 as its favored peer. The identification of favored 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 want a GSS to automatically query all mesh peers to find the closest up-to-date sticky database, leave the individual GSS device selection at `Unspecified`. The GSS uses the shortest round-trip time to prioritize which peers to request a database update.

7. Click the `Submit` button to save your DNS sticky configuration changes.

**Enabling Sticky in a DNS Rule**

This section contains the following topics:

- Sticky DNS Rule Overview
- Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups

**Note**

The DNS sticky global server load-balancing application is configurable only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable sticky in a DNS rule.

**Sticky DNS Rule Overview**

After you enable DNS sticky from the Global Sticky Configuration details page, add stickiness to a DNS rule using the DNS Rule Builder. The GSS supports DNS stickiness in a DNS rule on either a matching domain (By Domain) or on a matching domain list (By Domain List). The By Domain and By 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 also applies if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.
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.

**Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups**

To use the DNS Rule Builder 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 using the Global Sticky Configuration details page of the Traffic Mgmt tab. See the “Configuring DNS Sticky” section for details.

2. From the primary GSSM GUI, click the **DNS Rules** tab, and then click the **DNS Rules** navigation link. The DNS Rules list page appears.

3. Click the **Open Rule Builder** icon. The Create New DNS Rule page opens in a separate window.

4. Develop your DNS rule as outlined in steps 3 through 7 in the “Building DNS Rules Using the DNS Rule Builder” section of Chapter 7, Building and Modifying DNS Rules.

5. Enable or disable sticky globally for the DNS rule, at the Select Sticky Method option, by choosing one of the following selections:
   - **None**—Disables DNS sticky across the GSS network for this DNS rule. When you disable sticky, 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.
   - **By 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.
   - **By 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.

6. Override the global Entry Inactivity Timeout value set on the Global DNS Sticky details page (see the “Configuring DNS Sticky” section) for this DNS rule by specifying a value in the Inactivity Timeout field. Enter a value from 15 to 10080 minutes, defined in 5 minute intervals (15, 20, 25, 30, up to 10080).

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 inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database.

- **Note** The sticky inactivity timeout is accurate to within 5 minutes of the specified value. Each entry will persist 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.

7. At the Balance Clause 1 heading, perform the following:
Choose the answer group component of your first answer group and balance method pairing from the drop-down list. This is the first effort the GSS uses to select an answer for the DNS query.

Choose the balance method for the answer group from the drop-down list.

Click the Sticky Enable check box to activate DNS sticky for the balance clause. This checkbox appears only when you enable sticky for the DNS rule at the Select Sticky Method option.

8. Complete your DNS rule as described in the “Building DNS Rules Using the DNS Rule Builder” section of Chapter 7, Building and Modifying DNS Rules. Choose additional answer group and balance method pairings for Balance Clause 2 and Balance Clause 3.

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.

9. Click Save to save your DNS rule and return to the DNS Rules list page. The DNS rule is now active and processing incoming DNS requests.

Configuring Sticky Using the GSS CLI

This section describes how to configure a GSS device for DNS sticky operation from the CLI. From the primary GSSM CLI, you can obtain better scalability of your GSS DNS sticky configuration and allow sticky group creation through automated scripts. You can also use the CLI of each GSS in your network to perform sticky database activities on an individual GSS, such as removing sticky database entries from GSS memory, dumping entries from the sticky database to a named file, forcing an immediate backup of the sticky database, or loading and merging sticky database entries from a file.

The section contains the following topics:

- Logging in to the CLI and Enabling Privileged EXEC Mode
- Creating Sticky Groups
- Deleting Entries from the Sticky Database
- Dumping Sticky Database Entries
- Running a Periodic Sticky Database Backup
- Loading Sticky Database Entries

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

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

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

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

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

   gss1.example.com>

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

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

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

You 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 IPv4 and IPv6 addresses and subnet mask/prefix-length (in dotted-decimal notation for an IPv4 address and /n notation for an IPv6 address).

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. In this case, 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 IPv4 addresses from the CLI, you can configure a global netmask from the primary GSSM GUI 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 IPv4 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.
In addition to creating DNS sticky groups of multiple D-proxy IPv6 addresses from the CLI, you can configure a global netmask from the primary GSSM GUI to uniformly group contiguous D-proxies. The global prefix length 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 IPv6 address and the global prefix-length (range 1-128) as the key to look up in the DNS sticky database.

**Figure 9-1** illustrates 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 9-1  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.

You create sticky groups at the CLI of the primary GSSM to obtain better scalability of your configuration and to allow for ease of sticky group creation through automation 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 at 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/prefix-length]
```

The arguments and keywords are as follows:

- `groupname`—A unique alphanumeric name for the DNS sticky group. Contains a maximum of 80 characters. Use only alphanumeric characters and the underscore (_) character.
- `ip`—Specifies either an IPv4 or an IPv6 address block.
- `netmask`—Specifies the subnet mask of the IP address block. For an IPv4 address, enter the netmask in dotted-decimal notation, and for an IPv6 address, enter the netmask in an integer notation. For example, 255.255.255.0 is for IPv4 address and 2001:DB8:A:B::1 24 is for IPv6 address. The range of netmask for an IPv6 address is 1 - 128.

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 and 2001:DB8:A:B::1 64:

```
gssm1.example.com# config
sasl.example.com(config)# gslb
sasl.example.com(config-gslb)# sticky group StickyGroup1 ip 192.168.9.0 netmask 255.255.255.0
sasl.example.com(config-gslb)# sticky group StickyGroup1 ip 2001:DB8:A:B::1 netmask 128
```

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. For example, enter:

```
gssm1.example.com# config
sasl.example.com(config)# gslb
sasl.example.com(config-gslb)# no sticky group StickyGroup1 ip 192.168.3.0 netmask 255.255.255.0
sasl.example.com(config-gslb)# no sticky group StickyGroup1 ip 2001:DB8:A:B::1 netmask 128
```
Deleting a Sticky Group

You can delete a sticky group by using the no form of the sticky group command. For example, enter:

```
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 CLI 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 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 11, Monitoring GSS Global Server Load-Balancing Operation).

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 keywords and arguments 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 either an IPv4 or an IPv6 address of the sticky answer.

- **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. 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.
Valid entries are 0 to 10100 minutes.

- **ip ip_address netmask netmask**—Removes all sticky entries related to a D-proxy IP address and subnet mask. Specify either an IPv4 address or an IPv6 address of the requesting client’s D-proxy.

- **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:
```
gss1.example.com# sticky database delete ip 192.168.8.0 netmask 255.255.255.0
```
```
gss1.example.com# sticky database delete ip 2001:DB8:: netmask 112
```

## 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 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 do 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 arguments 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 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** CLI command.
  - **xml**—Dumps the assigned sticky entries in 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** CLI command. See Appendix B, “Sticky and Proximity XML Schema Files” for information on defining how content appears in output XML files.
Dumping sticky database 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 sticky database and the GSS platform in use. To avoid a degradation in performance, we recommend that you do not perform a sticky database dump in XML format during the routine operation of the GSS.

- **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. If the dump is large, progress messages appear.

```
# gss1.example.com

sticky database dump sdb2004_06_30 format xml entry-type ip
Starting Sticky Database dump.

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

sticky database dump sdb2004_06_30 format xml entry-type ip
Sticky 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 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 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:

```
# gss1.example.com

sticky database periodic-backup now
```

### Loading Sticky Database Entries

The database back-ups that are stored from the older software versions can be loaded into the software version 4.1(0) release using the same commands.
Chapter 9  Configuring DNS Sticky

Disabling DNS Sticky Locally on a GSS for Troubleshooting

The GSS supports the loading and merging of sticky database entries from a file into the existing sticky database in GSS memory. The sticky database merge capability supports the addition of entries from one GSS into 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 existing, 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 the 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:

```
gss1.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 GUI-enabled sticky option. You may need to locally disable sticky on a GSS when you need 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 GUI, the GSS reenables DNS sticky.

Use the **sticky stop** and **sticky start** commands to locally override the sticky enable option of the primary GSSM GUI.

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
- The 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 **gss 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 disk if a file is present and valid. Otherwise, the GSS starts with an empty sticky database.

This example shows how to locally disable DNS sticky on a GSS device using the **sticky stop** command:

```
gss1.example.com# sticky stop
```

This example shows how to locally reenable DNS on the GSS device using the **sticky start** command:

```
gss1.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 GUI
- Configuring Proximity Using the Primary GSSM GUI
- Configuring Proximity Using the GSS 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 11, Monitoring GSS Global Server Load-Balancing Operation, 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. 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 proximity probing agent, 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 contains 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 up to 32 zones. Within each zone, there is an active proximity probing agent that is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one proximity probing agent 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 proximity probing agent in a zone. Within each zone, there must be at least one proximity probing agent and, optionally, a backup proximity probing agent. If the primary proximity probing agent fails, the probes are redirected to the backup device. Once the primary proximity probing agent becomes available, probes are redirected back to the primary proximity probing agent.

The GSS uses Director Response Protocol (DRP) to communicate with the proximity probing agents (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. The GSS communicates with the proximity probing agent using the DRP RTT query and response method.
You can use another GSS as the proximity probing agent in a zone by enabling the DRP agent in the GSS. The GSS acting as a DRP agent supports ICMP, TCP, and path-probe RTT. You may also use any Cisco router as the proximity probing agent in a zone that can support the DRP agent software and measure ICMP or TCP; however, path-probe is not supported in the Cisco IOS router or other traditional DRP agent devices.

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 proximity probing agents in the GSS network, instructing the DRP agent in the proximity probing agent to probe specific D-proxy IP addresses. Each proximity probing agent 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 proximity probing agents to get proximity information between those proximity probing agents and the new D-proxy. After the GSS receives the probing results, it adds the RTT information to the PDB.

Figure 10-1 shows the probing process between a GSS (DRP client) and a proximity probing agent (DRP agent).

Figure 10-1  DRP Communication in a GSS Network
Network Proximity Overview

The GSS supports two types 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 proximity probing agents 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 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 proximity probing agents 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 proximity probing agents 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 (both dynamic and static). The GSS creates dynamic entries in the PDB as the result of requests for new D-proxy IP addresses. 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 include less probing activities performed by the GSS, less space required for the PDB, and 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 because 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 proximity probing agents in multiple zones to perform network proximity. See Figure 10-2 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 or smallest RTT metric. The DRP agent then returns the smallest RTT metric that identifies the closest zone, which in Figure 10-2 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 corresponding to 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.
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 are 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 proximity probing agent and, optionally, the backup proximity probing agent. Each proximity probing agent 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 proximity probing agent is the DRP agent located within the zone.

Each GSS network, or GSS mesh, can contain a maximum of sixteen GSS devices. GSS devices can be added and deleted 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 10-1** provides a quick overview of the steps required to configure the GSS for proximity network operation. Each step includes the primary GSSM GUI page or the GSS CLI command required to complete the task. For the procedures to configure the GSS for proximity, see the sections following the table.

**Table 10-1  Proximity Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>For example, enter:</td>
</tr>
<tr>
<td>gss1.example.com&gt; enable</td>
</tr>
<tr>
<td>gss1.example.com# config</td>
</tr>
<tr>
<td>gss1.example.com(config)# ntp-server 192.168.1.1 172.16.1.3</td>
</tr>
<tr>
<td>gss1.example.com(config)# ntp enable</td>
</tr>
<tr>
<td>2. Configure a Cisco router or GSS DRP agent in one or more proximity zones. For information about configuring the GSS as a DRP agent, see the <em>Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide</em>.</td>
</tr>
<tr>
<td>3. Log in to the primary GSSM GUI.</td>
</tr>
<tr>
<td>4. Click the <strong>Traffic Mgmt</strong> tab, and then click the <strong>Zone</strong> navigation link to access the Zones details page. Create one or more proximity zones in the Zones details page by specifying the index for the proximity zone, the IP address of the primary probe device, and the IP address of the backup probe device.</td>
</tr>
<tr>
<td>5. Click the <strong>Proximity</strong> navigation link to access the Proximity details page (Traffic Mgmt tab). At the State option, click the <strong>Enabled</strong> option button to globally enable proximity across the entire proximity network.</td>
</tr>
</tbody>
</table>
6. Modify one or more of the global proximity configuration default settings in the Proximity details page by performing the following steps:

- In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses. Use this parameter as an attempt to increase the number of Dproxies supported in the PDB. You can enter the mask in either dotted-decimal notation or as a prefix length in CIDR bit count notation.

- In the Entry Inactivity Timeout field, enter the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes the entry from the PDB.

- In the Equivalence Window field, enter a percentage value that the GSS applies to the most proximate RTT value to identify the relative RTT values of other zones that the GSS should consider as equally proximate. Use this parameter to adjust the granularity of the proximity decision process.

- In the Refresh Probe Interval field, enter the frequency of the refresh probing process to probe and update RTT values in the PDB.

- In the Initial Probe Method drop-down list, specify the type of probe method (TCP, ICMP, or path-probe) used initially by the Cisco IOS-based router during the probe discovery process of the requesting client’s D-proxy.

- In the Acceptable RTT field, enter a value that the GSS uses as the largest acceptable RTT value when determining the most proximate answer. Use this parameter to adjust the granularity of the proximity decision process.

- In the Acceptable Zone field, enter the minimum percentage of zones that the GSS requires to return RTT values before it returns a proximity answer. Use this parameter to adjust the granularity of the proximity decision process.

- In the Wait drop-down list, enable or disable the proximity wait state.

- In the DRP Authentication drop-down list, enable or disable DRP authentication.

7. If you enabled DRP Authentication and no DRP keys exist for the GSS, click the Add Proximity Key navigation link from the Proximity details page. Create one or more DRP keys in the Creating New DRP Key details page. Each DRP key includes a key identification number and a key authentication string. Click the Add button to save each DRP key.

8. Click the Submit button to save your global proximity configuration changes.

9. Associate a location to a proximity zone. Use either the Creating New Location details page for a new location or the Modifying Location details page for an existing location. Repeat this step if you have multiple locations that you want to assign to a proximity zone.

10. Assign a location that is associated with a proximity zone to an answer. Use either the Creating New Answer details page for a new answer or the Modifying Answer details page for an existing answer. Repeat this step if you have multiple answers that you want to assign to an associated proximity location.
Chapter 10      Configuring Network Proximity

11. Access the DNS Rules Builder as follows:
   a. Click the DNS Rules tab.
   b. Click the DNS Rules navigation link. The DNS Rules list appears.
   c. Click either the Open Rule Builder icon (if this DNS rule is new) or the Modify DNS Rule Using Rule Builder Interface icon (if this rule already exists) to access the DNS Rule Builder.

   Note
   You can configure the network proximity global server load-balancing application only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable proximity in a DNS rule.

12. Enable network proximity in a DNS rule by using the DNS Rule Builder. Define the DNS rule configuration information as follows:
   a. For each balance clause that is to perform proximity, click the Proximity Enable checkbox.
   b. To change the proximity acceptable RTT for the balance clause to a different value from the global proximity configuration, enter a value in the RTT field.
   c. To change the proximity acceptable zone for the balance clause to a different value from the global proximity configuration, enter a value in the Zone field.
   d. To change the proximity wait state to a different setting than the global proximity configuration, make a selection from the Wait drop-down list.

13. Log on to the CLI of a GSS in the network and enable privileged EXEC mode.

   gssm1.example.com> enable

14. (Optional) Group multiple D-proxy IP addresses as a single entry in the PDB to reduce probing and to take up less space in the PDB. You do so by accessing the global server load-balancing configuration mode, creating a proximity group at the primary GSSM CLI, and using the proximity group command to add multiple D-proxy IP addresses and subnet masks to the group.

   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
   or
   gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip 2001:DB8:1:1 netmask 24

15. (Optional) Add static proximity entries to the PDB of a GSS device in your network by accessing the global server load-balancing configuration mode and using the proximity assign command to create the static entries.

   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"
   or
   gssm1.example.com(config-gslb)# proximity assign group ISP2 zone-data "2001:DB8::1"

---

Table 10-1 Proximity Configuration Quick Start (continued)

Task and Command Example

11. Access the DNS Rules Builder as follows:
   a. Click the DNS Rules tab.
   b. Click the DNS Rules navigation link. The DNS Rules list appears.
   c. Click either the Open Rule Builder icon (if this DNS rule is new) or the Modify DNS Rule Using Rule Builder Interface icon (if this rule already exists) to access the DNS Rule Builder.

   Note
   You can configure the network proximity global server load-balancing application only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable proximity in a DNS rule.

12. Enable network proximity in a DNS rule by using the DNS Rule Builder. Define the DNS rule configuration information as follows:
   a. For each balance clause that is to perform proximity, click the Proximity Enable checkbox.
   b. To change the proximity acceptable RTT for the balance clause to a different value from the global proximity configuration, enter a value in the RTT field.
   c. To change the proximity acceptable zone for the balance clause to a different value from the global proximity configuration, enter a value in the Zone field.
   d. To change the proximity wait state to a different setting than the global proximity configuration, make a selection from the Wait drop-down list.

13. Log on to the CLI of a GSS in the network and enable privileged EXEC mode.

   gssm1.example.com> enable

14. (Optional) Group multiple D-proxy IP addresses as a single entry in the PDB to reduce probing and to take up less space in the PDB. You do so by accessing the global server load-balancing configuration mode, creating a proximity group at the primary GSSM CLI, and using the proximity group command to add multiple D-proxy IP addresses and subnet masks to the group.

   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
   or
   gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip 2001:DB8:1:1 netmask 24

15. (Optional) Add static proximity entries to the PDB of a GSS device in your network by accessing the global server load-balancing configuration mode and using the proximity assign command to create the static entries.

   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"
   or
   gssm1.example.com(config-gslb)# proximity assign group ISP2 zone-data "2001:DB8::1"
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 contains background information about choosing and configuring the Cisco router in each proximity zone as a DRP agent. It includes 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 the following:

- The DRP agent should be topologically close to each distributed server that it supports in the zone.
- The DRP agent in the Cisco IOS-based router can be 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 releases.

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”). “DRP Server Agent” and “ICMP ECHO-based RTT probing by DRP agents” are the Cisco IOS feature names as shown in the Cisco Feature Navigator II.

The following procedure summarizes how 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 the GSS device only. 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 the standard access list only.
4. If necessary, set up Message Digest (MD5) authentication with passwords as another security measure. You 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, it is important that you 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 failure occurs because the router does not 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. Together, 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 router as follows:

- To verify the DRP authentication configuration on the router running Cisco 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.
- To verify the DRP authentication configuration on the primary GSSM GUI, access the Global Proximity Configuration details page (Traffic Mgmt tab) and observe if the DRP Authentication selection is set to Enabled or Disabled (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 GUI and make them consistent to avoid a DRP authentication mismatch.

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. System clock changes 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 GUI. 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 “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, 192.168.1.1) 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:

```
gss1.example.com> enable
gss1.example.com# config
gss1.example.com(config)# ntp-server 192.168.1.1 172.16.1.3
gss1.example.com(config)# ntp enable
```

Creating Zones Using the Primary GSSM GUI

A proximity zone is a logical grouping of network devices that also contains one active proximity probing agent and a possible backup proximity probing agent. 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 the RTT data received from proximity probing agents configured in the zone. You can configure a proximity network with up to 32 zones.

This section contains the following topics:

- Creating a New Proximity Zone
- Modifying a Proximity Zone
- Deleting a Proximity Zone
- Associating a Proximity Zone with a Location
- Associating a Proximity-Based Location with an Answer

**Note**

Zone IP address can only be an IPv4. Proximity supports both IPv4 and IPv6 IP address requests for A and AAAA records.

Creating a New Proximity Zone

To create a new proximity zone from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zone** navigation link. The Zones list page appears.
3. Click the **Create Zone** icon. The Creating New Zone detail page appears.
4. In the Name field, enter an alphanumeric description of the zone. Only alphanumeric characters and the underscore (_) character are allowed.
5. In the Index field, specify the numerical identifier of the proximity zone. Enter an integer from 1 to 32. There is no default.
6. In the Probe Device field, enter the IP address of the primary probe device servicing this zone.
7. In the Backup Probe Device field, enter the IP address of the backup probe device for this zone.
8. Click the Submit button to save your zone. You return to the Zones list page.

**Modifying a Proximity Zone**

To modify a proximity zone from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the Traffic Mgmt tab.
2. Click the Zone navigation link. The Zones list page appears.
3. Click the Modify Zone icon located to the left of the zone that you want to modify. The Modifying Zone details page appears.
4. Use the fields provided to modify the zone configuration.

   **Note** The zone Index value cannot be modified. To change the zone index, delete the zone (see the “Deleting a Proximity Zone” section) and create a new zone that contains a different index.

5. Click Submit to save your configuration changes and return to the Zones list page.

**Deleting a Proximity Zone**

To delete a proximity zone from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the Traffic Mgmt tab.
2. Click the Zones navigation link. The Zones list page appears.
3. Click the Modify Zone icon located to the left of the zone that you want to delete. The Modifying Zone details page appears.
4. Click the Delete Zone icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the zone.
5. Click OK to confirm your decision and return to the Zones list page.

**Associating a Proximity Zone with a Location**

To associate a proximity zone with a location, perform the following steps:

1. From the primary GSSM GUI, click the Resources tab.
2. Click the Locations navigation link. The Locations list page appears.
3. Click either the Create Location icon (if this location is new) or the Modify Location icon (if you are adding the proximity zone to an existing location). The Location details page appears. For details about creating a location, see Chapter 2, Configuring Resources.
4. Click the Zone drop-down list and associate a zone with the location. There should be a logical connection between the zone and the location.
5. Click Submit to save changes to your location and return to the Locations list page.
**Associating a Proximity-Based Location with an Answer**

To assign a location that is associated with a proximity zone to an answer, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rule** tab.
2. Click the **Answers** navigation link. The Answers list page appears.
3. Click either the **Create Answer** icon (if this answer is new) or the **Modify Answer** icon (if you are adding the location to an existing answer). The Answer details page appears.
4. In the Type field, click the **VIP** option button. The VIP Answer section appears in the details page.
5. In the Name field, enter a name for the VIP-type answer that you are creating. Specifying a name for an answer is optional.
6. From the Location drop-down list, choose an appropriate GSS location that is associated with a proximity zone.
7. Complete the remaining VIP-type answer parameters as described in Chapter 6, Configuring Answers and Answer Groups.
8. Click **Submit** to save changes to your location and return to the Answers list page.
9. Repeat this procedure if you have multiple answers that you want to assign to an associated proximity location.

**Configuring Proximity Using the Primary GSSM GUI**

This section describes how to configure the GSS for network proximity from the primary GSSM GUI and how to add proximity to a DNS rule in the DNS Rule Builder. It contains the following topics:

- Configuring Proximity
- Creating DRP Keys
- Deleting DRP Keys
- Using the DNS Rule Builder to Add Proximity to a DNS Rule

**Configuring Proximity**

The GSS includes a set of proximity settings that function as the default values used by the GSS network when you enable proximity in a DNS rule. You enable proximity and modify the global proximity setting for the GSS network using the fields on the Global Proximity Configuration details page of the Traffic Mgmt tab. Changing a global proximity setting and applying that change is immediate and modifies the default values of the proximity settings used by the DNS Rule Builder.

To configure proximity from the primary GSSM GUI, perform the following steps:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears.
3. At the State option, click the **Enabled** option button to globally enable proximity across the entire GSS network. To globally disable proximity across the GSS network, click the **Disabled** option button.
4. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses in order to increase the number of supported D-proxies in the PDB. 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). The default global mask is 255.255.255.255.

When you define a proximity group for incoming D-proxy addresses (see the “Creating Proximity Groups” section), if the incoming D-proxy address does not match any of the entries in a defined proximity group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

5. In the Prefix length field, enter a global prefix length that the GSS uses to uniformly group contiguous D-proxy IPv6 address. By default, the value is set to 128.

When you define a proximity group for incoming D-proxy addresses (see the Cisco Global Site Selector Global Server Load-Balancing Configuration Guide, Chapter 9, Configuring Network Proximity), if the incoming D-proxy address does not match any of the entries in a defined proximity group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

6. In the Entry Inactivity Timeout field, enter the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry. Enter a value from 5 to 10080 minutes (168 hours).

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. The default value is 4320 minutes (72 hours).

7. In the Equivalence Window field, enter 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. Enter an equivalence window value from 0 to 100 percent.

Through the Equivalence Window percentage, you define an RTT window that the GSS uses to consider zones equal. The Equivalence Window 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 Window 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 Zone 1 and Zone 2 equally proximate in regards to the GSS selecting an answer. The RTT equivalence window range is from 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. The default value is 20 percent.

8. In the Refresh Probe Interval field, enter 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.

9. In the Initial Probe Method drop-down list, specify the type of probe method used initially by the Cisco IOS-based router or GSS DRP agent 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 ICMP, TCP, and path-probe as follows:
- TCP—The proximity probing agent uses the TCP SYN-ACK and RST handshake sequence to probe the user-specified TCP port and measure the RTT between the proximity probing agent and the D-proxy. You can configure the source and destination TCP ports on the Cisco router or GSS DRP agent.

- ICMP—The proximity probing agent uses ICMP echo request and response to measure the RTT between the proximity probing agent and the D-proxy.

- path-probe—This fallback method is used 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 proximity probing agents 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.

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 proximity probing agent and the D-proxy. The calculated path information is then sent back to the querying GSS.

Thus, 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.

10. In the Acceptable RTT field, enter a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. Enter an acceptable RTT value from 50 to 1500 ms. 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 parameter to adjust the granularity of the proximity decision process. The default value is 100 ms.

11. In the Acceptable Zone field, enter a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. Enter a percentage of zones from 3 to 100 percent.

   The Acceptable Zone 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 five different zones and you specify an Acceptable Zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of two 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. 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 GSS ignores the Acceptable Zone value.

12. In the Wait drop-down list, enter the GSS proximity wait-state condition:
   - Enabled—The GSS will 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.
   - Disabled—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. The GSS proceeds to the next balance clause in the DNS rule.

   The default setting is Disabled.

13. In the DRP Authentication drop-down list, enter the DRP authentication state as follows:
   - Enabled—The GSS authenticates packets that it exchanges with the DRP agent in a proximity probing agent through the exchange of DRP keys. The key authenticates the DRP requests and responses sent between the GSS and the DRP agent. You enable DRP authentication by creating a DRP key (see the “Creating DRP Keys” section).
   - Disabled—The GSS does not perform DRP authentication with the DRP agent.

   The default setting is Disabled.

14. Click the Submit button to save your global proximity configuration changes.

Creating DRP Keys

DRP supports the authentication of packets exchanged between the DRP agent (proximity probing agent) and the DRP client (the GSS). To enable DRP authentication for network proximity, create one or more DRP keys. Each DRP key contains a key identification number and a key authentication string. The primary GSSM GUI 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 proximity probing agent 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.

To create a DRP authentication key, perform the following steps:

1. From the primary GSSM GUI, click the Traffic Mgmt tab.
2. Click the Proximity navigation link. The Global Proximity Configuration details page appears.
3. Click the Add DRP Key navigation link. The Creating New DRP Key details page appears.
4. Enter the following values to create a DRP key:
   - ID—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. The range of key identification numbers is from 0 to 255.
Chapter 10 Configuring Network Proximity

### Configuring Proximity Using the Primary GSSM GUI

- **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 from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

5. Click the **Add** button to create your DRP authentication key.

6. Click the **Submit** button to save your global proximity configuration changes.

7. Repeat this procedure to create additional DRP keys. The primary GSSM supports a maximum of 32 keys.

### Deleting DRP Keys

To remove DRP authentication keys, perform the following steps:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.

2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears.

3. Click the **Remove DRP Key** navigation link. The Remove DRP Key details page appears.

4. Click the check box accompanying each DRP key that you want to remove from the list, and then click the **Remove Selected** button. The GSS removes the selected DRP keys from the page.

### Using the DNS Rule Builder to Add Proximity to a DNS Rule

After you configure network proximity from the primary GSSM GUI, add proximity to a DNS rule for VIP-type answer groups using the DNS Rule Builder. The balance method configured in the matched clause of the DNS rule determines which answer 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 list
- 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 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 proximity probing agents 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.
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.

To use the DNS Rule Builder to add proximity balance clauses to a DNS rule, perform the following steps:

1. From the primary GSSM GUI, click the **DNS Rules** tab, and then click the **DNS Rules** navigation link. The DNS Rules list page appears.

2. Click the **Open Rule Builder** icon. The Create New DNS Rule page opens in a separate window.

3. Develop your DNS rule as outlined in Steps 3 through 8 in the “Building DNS Rules Using the DNS Rule Builder” section of Chapter 7, Building and Modifying DNS Rules.

4. At the Balance Clause 1 heading, perform the following:
   - Choose the answer group component of your first answer group and balance method pairing from the drop-down list. This is the first effort performed by the GSS to select the most proximate answer for the DNS query. Ensure that the answers in the answer group are contained in locations that are tied to a zone.
   - Choose the balance method for the answer group from the drop-down list.

5. Specify the following proximity parameters as part of the DNS rule balance clause:
   - **Proximity Enable**—To activate network proximity for the balance clause, click the Proximity Enable checkbox. This checkbox appears only when the answers in the answer group are contained in locations that are tied to a zone.
   - **RTT**—To change the proximity-acceptable RTT for the balance clause to a different value from the global proximity configuration, enter a value in the RTT field. Enter an acceptable RTT value from 50 to 1500 ms.
     - The GSS uses this value as the user-specified acceptable RTT 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 one of the following:
       - Disregards the acceptable percentage of zones.
       - Considers that there is sufficient proximity data to make a proximity decision.
       - Uses the zones reporting less than or equal to this value in a proximity decision.
     - The default value is 100 ms.
   - **Zone**—To change the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration, enter a value in the Zone field. Enter a percentage of zones from 3 to 100 percent.
     - The Acceptable Zone 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 criterion. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.
     - The default value is 40 percent.
• Wait—To change the proximity wait state to a different setting than the global proximity configuration, make a selection from the drop-down list. Enter the GSS proximity wait state condition as follows:
  – Default—Always use the globally defined proximity wait state.
  – Enabled—The GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. While the GSS waits for sufficient proximity data, it does not return an answer to the requesting client’s D-proxy until the GSS obtains sufficient proximity data to complete the selection process.
  – Disabled—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.

6. Repeat Steps 4 and 5 to choose additional answer group and balance method pairings for Balance Clause 2 and Balance Clause 3.

7. Click Save to save your DNS rule and return to the DNS Rules list page. The DNS rule is now active and processing incoming DNS requests.

Configuring Proximity Using the GSS CLI

This section describes how to configure a GSS device for network proximity from the CLI. From the primary GSSM CLI, you can create proximity groups to obtain better scalability of your GSS proximity configuration and to allow for ease of proximity group creation through automation scripts. You can also use the CLI of each GSS in your proximity network to perform PDB activities on an individual GSS basis, such as configuring static proximity entries, removing PDB entries from GSS memory, dumping entries from the PDB to a named file, forcing an immediate backup of the PDB, or loading and merging PDB from a file.

The section contains the following topics:

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

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

1. Power on your GSS. After the GSS boot process completes, the software prompts you to log in to the device.
2. If you are remotely logging in to the GSS device (GSS or GSSM) through Telnet or SSH, enter the hostname or IP address of the GSS to access the CLI.

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

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

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

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

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

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

**Creating Proximity Groups**

This section contains the following topics:

- Proximity Group Overview
- Creating a Proximity Group
- 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 the following:

- 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 GUI 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 10-3 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 10-3  Locating a Grouped Proximity Database Entry

Creating a Proximity Group

You can create a proximity group by using the **proximity group** global server load-balancing configuration mode command from the primary GSSM CLI. This command allows you 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.

You create proximity groups at the CLI of the primary GSSM to obtain better scalability of your configuration and to allow for easy proximity group creation through automated scripts. The proximity groups are saved in the primary GSSM database and 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 keywords and arguments are as follows:

- **groupname**—A unique alphanumeric name for the proximity group that contains a maximum of 80 characters. Use only alphanumeric characters and the underscore (_) character.
- **ip ip-address**—Specifies the IP address block in dotted-decimal notation (for example, 192.168.9.0).
Chapter 10  Configuring Network Proximity

Configuring Proximity Using the GSS CLI

- **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.

### 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)# gslb
gssm1.example.com(config-gslb)# 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 proximity probing agents 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 new, assigned entry. You can use automated scripts if you intend to add numerous static entries in the PDB of each GSS.
You can also successfully add static proximity entries on the primary GSS. However, you cannot add entries by zone on any other GSS. When you attempt to use static entries locally and configure them separately on each GSS using the `proximity assign` CLI command, the GSS responds that this command is valid only on the primary GSSM.

**Note**
Be aware that the `proximity assign` CLI command affects only the local GSS. The configuration is not synchronized with the other GSSs in the network.

Static entries in the PDB do not age out. They remain in the PDB until you delete them. In addition, static entries are not subject to the automatic database cleanup of the least recently used entries when the PDB size is almost at the maximum number of entries. Use the `no` form of the `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 proximity probing agents 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 long. Ensure that the `proximity assign` command does not exceed that length when you configure RTT for a large number of proximity zones.

The keywords and arguments are as follows:

- **group groupname**— Specifies a unique alphanumeric name for a group of static entries with a maximum of 16 characters. Use only alphanumeric characters and the underscore (_) character. 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 to probe by the proximity probing agent. The proximity probing agent 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 proximity probing agent, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.

- **zone-data “zonelId:RTT”**— (Optional) Specifies the calculated RTT value for a zone, specified in “zonelId:RTT” format. For example, enter "1:100" to specify zone 3 with an RTT of 100 seconds. Valid entries for `zonelId` are from 1 to 32, and must match the proximity zone index specified through the primary GSSM GUI (see the “Synchronizing the GSS System Clock with an NTP Server” section). Valid entries for the `RTT` value are from 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:

```
gssml.example.com# config
 gssml.example.com(config)# gslb
 gssml.example.com(config-gslb)# proximity assign group ISP1 probe-target 192.168.2.2
 or
 gssml.example.com(config-gslb)# proximity assign group ISP1 probe-target 2001:DB8::1
```
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 GUI:

```
(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 through the CLI. To delete static entries from the PDB in 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` form of the `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 GSS memory by using the `proximity database delete` CLI command. However, this command 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 keywords and arguments are as follows:

- **all**—Removes all proximity database entries from 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.
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:

```plaintext
gss1.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 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 types 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:

```plaintext
proximity database dump [filename] format {binary | xml} [entry-type {all | assigned | probed}] [entry-address {ip-address | netmask {netmask}}]
```

The keywords and arguments are as follows:
Chapter 10 Configuring Network Proximity

Configuring Proximity Using the GSS CLI

- **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 CLI command.
  - **xml**—Dumps the assigned proximity entries in XML format. The contents of an XML file includes the data fields along with the data descriptions. The contents of this file can be viewed using the type CLI 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. We recommend that you do not perform a PDB dump in XML format during the routine operation of the GSS to avoid a degradation in performance.

- **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.
  - **assigned**—Dumps statically assigned proximity entries.
  - **probed**—Dumps dynamically probed proximity entries.

The default is **all**.

- **entry-address ip-address**—Specifies the IP address of the PDB entry. Both IPv4 and IPv6 are supported.
- **netmask netmask**—Specifies the subnet mask of the PDB entry (for example, for an IPv4 address the subnet mask is 255.255.255.0 and for an IPv6 address the subnet is /64).

This example shows how to dump the dynamic PDB entries to a file named PDB2004_6_30 in XML format. If the dump is large, progress messages appear.

```bash
GSS1.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.

GSS1.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

GSS1.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.

The syntax for this command is as follows:

```
proximity database periodic-backup now
```

For example, enter:

```
gss1.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 keywords and arguments are as follows:

- `filename`—The 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 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 take 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:

```
gss1.example.com# proximity database load file GSS3PDB format binary
```
For example, to override the same entries located in the existing GSS PDB, enter:

gss1.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.

When you need to instruct the proximity probing agent 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 keywords and arguments are as follows:

- **dproxy_address**—IP network address of the D-proxy that you want to probe from the proximity probing agent. The D-proxy address can either be an IPv4 or an IPv6 address.
- **zone zoneId**—Specifies the ID of the proximity zone containing the proximity probing agent from which you want to initiate a probe. Available values are from 1 to 32.
- **all**—Specifies that the GSS instructs the proximity probing agents in all configured zones to transmit a probe to the specified D-proxy IP address.

For example, to instruct the proximity probing agent in zone 1 to send a probe to the D-proxy at 172.16.5.7, enter:

gss1.example.com# proximity probe 172.16.5.7 zone 1

For example, to instruct the proximity probing agent in zone 1 to send a probe to the D-proxy at 2001:DB8:A:B::1, enter:

gss1.example.com# proximity probe 2001:DB8:A:B::1 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 GUI-enabled proximity option. You may need to locally disable proximity on a GSS when you need 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:

```
gss1.example.com# proximity stop
```

This example shows how to locally reenable proximity on a GSS device using the `proximity start` command:

```
gss1.example.com# proximity start
```

Where to Go Next

Chapter 11, Monitoring GSS Global Server Load-Balancing Operation, 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.
Monitoring GSS Global Server Load-Balancing Operation

This chapter describes the following tools for monitoring 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:

- Monitoring Global Server Load-Balancing Statistics from the CLI
- Monitoring Global Load-Balancing Statistics from the Primary GSSM GUI

Monitoring 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, you can use the show statistics dns command to view 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 monitor 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 monitor GSS global server load-balancing operation.

- Monitoring the Status of the Boomerang Server on a GSS
- Monitoring the Status of the DNS Server on a GSS
- Monitoring the Status of the DRP Agent on a GSS
- Monitoring DDoS Statistics on a GSS
- Monitoring the Status of Keepalives on a GSS
- Monitoring Network Proximity Statistics on a GSS
Monitoring Global Server Load-Balancing Statistics from the CLI

Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

- Monitoring DNS Sticky Statistics on a GSS
- Clearing GSS Global Server Load-Balancing Statistics

Monitoring the Status of the Boomerang Server on a GSS

The boomerang server component uses calculations of network delay, provided by DNS races between CRAs, to determine which server is best able to respond to a given request. You use the `show statistics boomerang` command to view boomerang activity, such as DNS races, on your GSS device on a domain-by-domain basis or on a global basis.

The syntax of this 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 display 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 display boomerang statistics for a specific domain:

```
gss1.yourdomain.com# show statistics boomerang domain1
Domain statistics: (of domain1)
  DNS A requests:
```

Monitoring 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. You use the `show statistics dns` command option to view 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 viewing the DNS answer group, domain list, or source address list statistics, you may specify the `verbose` option to view 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 Statistics for all GSSs in the GSS Mesh
- Displaying Answer Group Statistics
- Displaying Domain Statistics
- Displaying Domain List Statistics
- Displaying Global Statistics
- Displaying DNS Rule Proximity Statistics
• Displaying DNS Rule Statistics
• Displaying DNS Rule Statistics for all GSSs in the GSS Mesh
• 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 entering 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 of this command is as follows:

```
show statistics dns answer [list | verbose | answer_name]
```

The keywords and arguments are as follows:

- `list`—(Optional) Lists the names of all answers configured for the GSS.
- `verbose`—(Optional) Allows you to display detailed statistics for each answer. In addition to the information that displays when you do not use an optional keyword, the DNS name also displays.
- `answer_name`—(Optional) Name of the answer that you want to display statistics.

Table 11-1 describes the fields in the `show statistics dns answer` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Answer           | Name of the answer. Depending on the type of answer, the GSS displays the following:  
|                  | • 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. |
| 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 Statistics for all GSSs in the GSS Mesh

From the primary GSSM, you can display answer statistics for all of the online GSS devices in the GSS mesh by using the `show statistics gss-mesh all dns answer` command. For every online GSS, the primary GSSM displays the accumulated hit count for each configured answer that responds to content queries.

The syntax of this command is as follows:

```
show statistics gss-mesh all dns answer [type {cra | ns | vip}] [ip_address]
```

The keywords and arguments are as follows:

- **type**—(Optional) Specifies statistics for one of the following answer types:
  - `cra`—Content routing agent answer type
  - `ns`—DNS name server answer type
  - `vip`—Virtual IP answer type
- **ip_address**—(Optional) IP address of a specific GSS in the GSS mesh.

Table 11-2 describes the fields in the `show statistics gss-mesh all dns answer` command output.

**Table 11-2 Field Descriptions for show statistics gss-mesh all dns answer Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the GSS in the GSS mesh.</td>
</tr>
<tr>
<td>Name</td>
<td>Answer name.</td>
</tr>
<tr>
<td>Type</td>
<td>Resources to which the GSS resolves DNS requests. The answer types include VIP, CRA, or Name Server (NS).</td>
</tr>
</tbody>
</table>
| Status | Answer status. Possible states are as follows:  
  - Online—Indicates that the answer is online and can be used by any of the currently configured DNS rules.  
  - Offline—Indicates that the answer is offline and cannot be used by any of the currently configured DNS rules.  
  - Suspended—Indicates that the answer is administratively suspended and cannot be used by any of the currently configured DNS rules.  
  - Operational Suspend—Indicates that the GSS has suspended the answer because it was offline and the manual-reactivation option was enabled on the answer. For this state to display, you must have the global manual reactivation feature enabled on the primary GSSM.  
  - Unknown—Indicates that the primary GSSM was recently restarted and is waiting for an answer status from its peer GSS. |
| Hit Count | Total number of hits for the configured answer since the GSS was last started or statistics cleared. |

Displaying Answer Group Statistics

You display the total hit count for each configured answer group and the answers contained in the answer group by entering the `show statistics dns answer-group` command.
The syntax of this 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 view statistics.
- `verbose`—Allows you to view detailed statistics for each answer that makes up an answer group.

Table 11-3 describes the fields in the `show statistics dns answer-group verbose` command output.

### Table 11-3 Field Descriptions for `show statistics dns answer-group verbose` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hit Count</td>
<td>Accumulated hit count for the configured answer group since the GSS was last started.</td>
</tr>
<tr>
<td>Answer</td>
<td>Name of each answer in the answer group. Depending on the type of answer, the GSS displays the following:</td>
</tr>
<tr>
<td></td>
<td>- VIP address of the answer (VIP-type answer)</td>
</tr>
<tr>
<td></td>
<td>- Interface or circuit address (CRA-type answer)</td>
</tr>
<tr>
<td></td>
<td>- IP address of the name server (Name Server-type answer)</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times that the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the answer is online (up) or offline (down).</td>
</tr>
</tbody>
</table>

### Displaying Domain Statistics

You display the accumulated hit count for each configured host domain by entering 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 of this 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 view statistics.

Table 11-4 describes the fields in the `show statistics dns domain` command output.

### Table 11-4 Field Descriptions for `show statistics dns domain` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Name of the hosted domain.</td>
</tr>
<tr>
<td>Total Hits</td>
<td>Total number of hits for the specified hosted domain since the GSS was last started.</td>
</tr>
<tr>
<td>1-Min</td>
<td>Averaged per second hit count for the hosted domain, calculated during the last minute.</td>
</tr>
</tbody>
</table>
Displaying Domain List Statistics

You display the total accumulated hit count for each configured domain list by entering the `show statistics dns domain-list` command.

The syntax of this 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`—Specifies the name of the domain list that you want to view statistics.
- `verbose`—Allows you to view detailed statistics for each domain that makes up a domain list.

Table 11-5 describes the fields in the `show statistics dns domain-list verbose` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hit Count</td>
<td>Accumulated hit count for the hosted domain since the GSS was last started or statistics cleared.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the hosted domain in the domain list.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times that the hosted domain has been selected or matched in the DNS rule when the GSS processes a DNS request.</td>
</tr>
</tbody>
</table>

Displaying Global Statistics

You display general DNS statistics for the GSS device in use by entering the `show statistics dns global` command.

The syntax of this command is as follows:

```
show statistics dns global
```

Table 11-6 describes the fields in the `show statistics dns global` command output.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DnsQueriesRcvd</td>
<td>Total number of DNS queries received by the GSS from a requesting client D-proxy.</td>
</tr>
<tr>
<td>DnsHostAddrQueriesRcvd</td>
<td>Total number of host address queries received by the GSS from a requesting client D-proxy.</td>
</tr>
<tr>
<td>DnsResponsesSent</td>
<td>Total number of DNS responses sent by the GSS to a requesting client D-proxy.</td>
</tr>
<tr>
<td>DnsResponsesNoError</td>
<td>Total number of DNS responses sent by the GSS to a requesting client D-proxy without an error.</td>
</tr>
<tr>
<td>DnsResponsesErrors</td>
<td>Total number of DNS responses sent by the GSS to a requesting client D-proxy with an error.</td>
</tr>
<tr>
<td>DnsServfailRCode</td>
<td>DNS server failure return code.</td>
</tr>
<tr>
<td>DnsNxdomainRCode</td>
<td>DNS NX domain return code.</td>
</tr>
<tr>
<td>DnsNotimpRCode</td>
<td>DNS not implemented return code.</td>
</tr>
<tr>
<td>DnsRefusedRCode</td>
<td>DNS refused return code.</td>
</tr>
<tr>
<td>DnsQueriesUnmatched</td>
<td>Total number of unmatched DNS queries received by the GSS from a requesting client D-proxy.</td>
</tr>
<tr>
<td>DnsDrops</td>
<td>Total number of DNS queries dropped by the GSS.</td>
</tr>
<tr>
<td>DnsNSFWDSent</td>
<td>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.</td>
</tr>
<tr>
<td>DnsBoomServReqSent</td>
<td>Total number of requests sent by the boomerang server in the GSS to initiate a DNS race.</td>
</tr>
<tr>
<td>DnsNSFWDResponsesRcvd</td>
<td>Total number of queries that have been forwarded to the GSS to an external DNS name server for resolution.</td>
</tr>
<tr>
<td>DnsProxLkupReqSent</td>
<td>Total number of proximity lookup requests sent by the selector to the proximity subsystem.</td>
</tr>
<tr>
<td>DnsProxLkupRespRecd</td>
<td>Total number of proximity lookup requests received by the selector from the proximity subsystem.</td>
</tr>
<tr>
<td>DnsReqRatePerSecondCur</td>
<td>Current request rate per second that requests are made to the GSS to perform a DNS resolution.</td>
</tr>
<tr>
<td>DnsReqRatePerSecondPeak</td>
<td>Peak request rate per second that requests are made to the GSS to perform a DNS resolution.</td>
</tr>
<tr>
<td>DnsStickyLkupReqSent</td>
<td>Total number of sticky lookup requests sent by the selector to the sticky subsystem.</td>
</tr>
<tr>
<td>DnsStickyAddReqSent</td>
<td>Total number of requests for IP addresses sent by the selector to the sticky subsystem.</td>
</tr>
<tr>
<td>DnsStickyHit</td>
<td>Total number of successful sticky answer matches for the DNS rule.</td>
</tr>
<tr>
<td>DnsStickyMiss</td>
<td>Total number of times that the GSS was unable to provide the sticky answer for the DNS rule.</td>
</tr>
<tr>
<td>DnsSrcPortErrorUdp</td>
<td>Total number of UDP errors that occurred on the DNS source port.</td>
</tr>
</tbody>
</table>
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

Displaying DNS Rule Proximity Statistics

You display all proximity lookups by DNS rule name by entering the `show statistics dns proximity rule` command.

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 of this command is as follows:

```
show statistics dns proximity rule
```

Table 11-7 describes the fields in the `show statistics dns proximity rule` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Name of the matched DNS rule.</td>
</tr>
<tr>
<td>Proximity Hit Count</td>
<td>Number of DNS requests that match the DNS rule.</td>
</tr>
<tr>
<td>Proximity Success Count</td>
<td>Number of DNS responses successfully returned with a proximate answer for the DNS rule.</td>
</tr>
</tbody>
</table>

Displaying DNS Rule Statistics

You display the total hit count and success count for each configured DNS rule by entering the `show statistics dns rule` command.

The syntax of this command is as follows:

```
show statistics dns rule [list | rule_name [verbose]]
```

The keywords and arguments are as follows:

- `list`—(Optional) Lists the names of all DNS rules configured for the GSS.
- `rule_name`—(Optional) Name of the DNS rule that you want to display statistics.
- `verbose`—(Optional) Allows you to display detailed statistics for the specified rule.

Table 11-8 describes the fields in the `show statistics dns rule rule_name verbose` command output.
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

Table 11-8  Field Descriptions for show statistics gss-mesh all dns rule verbose Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hit Count</td>
<td>Accumulated hit count for the configured DNS rule since the GSS was last started.</td>
</tr>
<tr>
<td>Total Success Count</td>
<td>Accumulated number of successful answer matches for the DNS rule.</td>
</tr>
<tr>
<td>Clause</td>
<td>Number of the balance clause in the DNS rule.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of times that the DNS rule processed a DNS request.</td>
</tr>
<tr>
<td>Success Count</td>
<td>Number of successful answer matches for the DNS rule.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the clause. The possible states are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active—Indicates that the clause is active.</td>
</tr>
<tr>
<td></td>
<td>• Suspended—Indicates that the clause is administratively suspended.</td>
</tr>
<tr>
<td></td>
<td>• Operational Suspend—Indicates that the GSS has suspended the clause</td>
</tr>
<tr>
<td></td>
<td>because it was offline and the manual-reactivation option was enabled on</td>
</tr>
<tr>
<td></td>
<td>the clause. For this state to display, you must have the global manual</td>
</tr>
<tr>
<td></td>
<td>reactivation feature enabled on the primary GSSM.</td>
</tr>
<tr>
<td>Id</td>
<td>Internal ID number of the answer in the DNS rule.</td>
</tr>
<tr>
<td>Address</td>
<td>Name of the answer. Depending on the type of answer, the GSS displays the following:</td>
</tr>
<tr>
<td></td>
<td>• VIP address of the answer (VIP-type answer)</td>
</tr>
<tr>
<td></td>
<td>• Interface or circuit address (CRA-type answer)</td>
</tr>
<tr>
<td></td>
<td>• IP address of the name server (Name Server-type answer)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit Count</td>
<td>Number of times that the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.</td>
</tr>
</tbody>
</table>

### Displaying DNS Rule Statistics for all GSSs in the GSS Mesh

From the primary GSSM, you can display rule statistics for all of the online GSS devices in the GSS mesh by using the `show statistics gss-mesh all dns rule` command. For every online GSS, the primary GSSM displays the total hit counts and success counts for each configured DNS rule.

The syntax of this command is as follows:

```
show statistics gss-mesh all dns rule [rule_name]
```

The optional `rule_name` argument is the name of the DNS rule that you want to display statistics. Table 11-8 describes the fields in the `show statistics gss-mesh all dns rule` command output.

Table 11-9  Field Descriptions for show statistics gss-mesh all dns rule Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS rule name</td>
<td>Name of the DNS rule.</td>
</tr>
<tr>
<td>Total Hits</td>
<td>Accumulated hit count for the configured DNS rule since the GSS was last started.</td>
</tr>
<tr>
<td>Successful hits</td>
<td>Accumulated number of successful answer matches for the DNS rule.</td>
</tr>
</tbody>
</table>
Displaying Source Address Statistics

You display the accumulated hit count for each configured source address by entering the `show statistics dns source-address` 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 of this 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 view statistics.

Table 11-10 describes the fields in the `show statistics dns source-address` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src Address</td>
<td>IP address or CIDR address block of the client DNS proxy.</td>
</tr>
<tr>
<td>Total Hits</td>
<td>Total number of hits for the source address since the GSS was last started or statistics cleared.</td>
</tr>
<tr>
<td>1-Min</td>
<td>Averaged per second hit count for the source address, calculated during the last minute.</td>
</tr>
<tr>
<td>5-Min</td>
<td>Averaged per second hit count for the source address, calculated during the last 5-minute interval.</td>
</tr>
<tr>
<td>30-Min</td>
<td>Averaged per second hit count for the source address, calculated during the last 30-minute interval.</td>
</tr>
<tr>
<td>4-Hr</td>
<td>Averaged per second hit count for the source address, calculated during the last 4-hour interval.</td>
</tr>
</tbody>
</table>

Displaying Source Address List Statistics

You display the total hit count for each configured source address list by entering 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 of this 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 view statistics.
- **verbose**—Allows you to view detailed statistics for each name in the source address list.

Table 11-11 describes the fields in the `show statistics dns source-address-list` command output.
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

Displaying DNS Rule Sticky Statistics

You display all DNS sticky lookups by DNS rule name by entering the `show statistics dns sticky rule` command.

Note
To clear sticky 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 of this command is as follows:

```
show statistics dns sticky rule
```

Table 11-12 describes the fields in the `show statistics dns sticky rule` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Name of the matched DNS rule.</td>
</tr>
<tr>
<td>Sticky Hit Count</td>
<td>Total number of lookups in the sticky database for the DNS rule.</td>
</tr>
<tr>
<td>Sticky Success Count</td>
<td>Total number of successful sticky answer matches for the DNS rule.</td>
</tr>
</tbody>
</table>

Monitoring the Status of the DRP Agent on a GSS

You monitor statistics on the Director Response Protocol (DRP) agent by entering the `show statistics drpagent` command.

Note
To clear statistics related to the DRP agent component of the GSS, use the `clear statistics drpagent` command. See the “Clearing GSS Global Server Load-Balancing Statistics” section for details.

The syntax of this command is as follows:

```
show statistics drpagent
```

Table 11-13 describes the fields in the `show statistics drpagent` command output.
Monitoring DDoS Statistics on a GSS

This section describes the procedures you need to follow to display DDoS statistics from the CLI and contains the following topics:

- Displaying DDoS Attack Statistics
- Displaying DDoS Anti-Spoofing Statistics
- Displaying DDoS Failed DNS Queries
- Displaying DDoS Rate-Limit Values
- Displaying the DDoS Running Configuration
- Displaying DDoS Statistics
- Displaying DDoS Status

Displaying DDoS Attack Statistics

You display the DNS attacks detected by the GSS by entering the `show ddos attacks` command (from privileged EXEC mode) or the `show attacks` command (from ddos configuration mode).

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

Note that only IPv4 traffic is supported.

The syntax of this command is as follows:
show [ddos] attacks

Table 11-14 describes the fields in the show [ddos] attacks command output.

Table 11-14 Field Descriptions for show [ddos] attacks Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Attacks</td>
<td>Total number of DNS attacks detected by the GSS.</td>
</tr>
<tr>
<td>Reflection attack</td>
<td>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.</td>
</tr>
<tr>
<td>Malformed DNS packet attacks</td>
<td>Attack in which the GSS is flooded with malformed DNS packets.</td>
</tr>
<tr>
<td>Failed Global Domain attacks</td>
<td>Failed domain counter provides a total for DNS queries that failed to match the global domain name.</td>
</tr>
<tr>
<td>Global Rate-limit exceeded attacks</td>
<td>Attack in which the maximum number of DNS requests that the GSS receives from the D-proxy per second exceeds the global limit.</td>
</tr>
</tbody>
</table>

For example, enter:

```plaintext
[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 entering the show ddos dproxy command (from privileged EXEC mode) or the show dproxy command (from ddos configuration mode).

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 of this 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 11-15 describes the fields in the show [ddos] dproxy command output.
Displaying DDoS Failed DNS Queries

You display the following by entering the `show ddos failed-dns` command (from privileged EXEC mode) or the `show failed-dns` command (from ddos configuration mode):

- 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 see DNS queries for a domain not configured on the GSS.

Table 11-15 Field Descriptions for `show [ddos] d-proxy` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dproxy Address</td>
<td>IP address of the D-proxy.</td>
</tr>
<tr>
<td>Spoofed/Nonspoofed</td>
<td>Spoofed or nonspoofed D-proxy.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of dropped packets due to anti-spoofing failure.</td>
</tr>
</tbody>
</table>

For example, enter:

```
gssm1.example.com# show ddos dproxy 16.1.1.11
```

<table>
<thead>
<tr>
<th>DPROXY ADDRESS</th>
<th>SPOOFED/NONSPOOFEDDROPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1.1.11</td>
<td>Spoofed 3</td>
</tr>
</tbody>
</table>

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 of this command is as follows:

```
```

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`—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 11-16 describes the fields in the `show [ddos] failed-dns` command output.

Table 11-16 Field Description for `show [ddos] failed-dns` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global domain check drops</td>
<td>Number of dropped packets as a result of a global domain name check.</td>
</tr>
</tbody>
</table>
### Displaying DDoS Rate-Limit Values

You display the rate limits per D-proxy and the number of packets dropped per source by entering the `show ddos rate-limit` command (from privileged EXEC mode) or the `show rate-limit` command (from ddos configuration mode).

The syntax of this 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 11-17 describes the fields in the `show [ddos] rate-limit` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dproxy Address</td>
<td>IP address of the D-proxy.</td>
</tr>
<tr>
<td>Rate-limit</td>
<td>Maximum number of DNS requests that the GSS can receive from a D-proxy per second.</td>
</tr>
<tr>
<td>Applied Rate Limit</td>
<td>This value is based on the following:</td>
</tr>
<tr>
<td></td>
<td>rate-limit * scaling factor/100</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of packets dropped because of the rate-limit.</td>
</tr>
</tbody>
</table>

For example, enter:

```gssm1.example.com# show ddos rate-limit
Global domain check drops:4
```

### Table 11-16 Field Description for show [ddos] failed-dns Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dproxy Address</td>
<td>IP address of the D-proxy.</td>
</tr>
<tr>
<td>Number of Failed DNS queries</td>
<td>Number of failed DNS queries as a result of a GSLB-rule check.</td>
</tr>
</tbody>
</table>

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 entering the `show ddos rate-limit` command (from privileged EXEC mode) or the `show rate-limit` command (from ddos configuration mode).

The syntax of this 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 11-17 describes the fields in the `show [ddos] rate-limit` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dproxy Address</td>
<td>IP address of the D-proxy.</td>
</tr>
<tr>
<td>Rate-limit</td>
<td>Maximum number of DNS requests that the GSS can receive from a D-proxy per second.</td>
</tr>
<tr>
<td>Applied Rate Limit</td>
<td>This value is based on the following:</td>
</tr>
<tr>
<td></td>
<td>rate-limit * scaling factor/100</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of packets dropped because of the rate-limit.</td>
</tr>
</tbody>
</table>
### Displaying the DDoS Running Configuration

You display the contents of the DDoS running configuration file by entering the `show ddos-config` command (from privileged EXEC or ddos configuration mode).

The syntax of this command is as follows:

```
show ddos-config
```

**Table 11-18** describes the fields in the `show ddos-config` command output.

**Table 11-18 Field Descriptions for show ddos-config Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>DDoS detection and mitigation module status, enabled or disabled.</td>
</tr>
<tr>
<td>rate-limit global</td>
<td>Global rate limit configured on the GSS.</td>
</tr>
<tr>
<td>tolerance factor</td>
<td>Helps determine the rate limit.</td>
</tr>
<tr>
<td>peacetime database</td>
<td>Peacetime database identifier.</td>
</tr>
<tr>
<td>global domain</td>
<td>Global domain name identifier.</td>
</tr>
<tr>
<td>dproxy trusted</td>
<td>D-proxy added or deleted from a trusted D-proxy database.</td>
</tr>
<tr>
<td>mitigation-rule response</td>
<td>Enables mitigation rules for the following DNS responses:</td>
</tr>
<tr>
<td>enable</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.</td>
</tr>
<tr>
<td>mitigation-rule request</td>
<td>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).</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
</tbody>
</table>

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 16.1.1.12 40
 rate-limit 16.1.1.11 40
 mitigation-rule response enable
 mitigation-rule request enable
```
Displaying DDoS Statistics

You display DDoS statistics by entering the `show statistics ddos` command (from privileged EXEC mode), or the `show statistics` command (from ddos configuration mode).

**Note**

Clear statistics related to the DDoS detection and mitigation component of the GSS by entering the `clear statistics ddos` command. See the “Clearing GSS Global Server Load-Balancing Statistics” section for details.

The syntax of this command is as follows:

```plaintext
show statistics [ddos] [attacks | global]
```

The keywords and arguments are as follows:
- `attacks`—Displays attack statistics.
- `global`—Displays global statistics.

Table 11-19 describes the fields in the `show statistics ddos attacks` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Attacks</td>
<td>Total number of DDoS attacks on the GSS.</td>
</tr>
<tr>
<td>Reflection attacks</td>
<td>Attack in which the IP address of the victim (that is, the GSS) is spoofed</td>
</tr>
<tr>
<td></td>
<td>and multiple DNS requests are sent to a DNS server or multiple DNS servers</td>
</tr>
<tr>
<td></td>
<td>posing as the victim.</td>
</tr>
<tr>
<td>Malformed DNS packet</td>
<td>Attack in which the GSS is flooded with malformed DNS packets.</td>
</tr>
<tr>
<td>attacks</td>
<td></td>
</tr>
<tr>
<td>Failed Global Domain</td>
<td>Attack in which the GSS is flooded with failed global domain attacks.</td>
</tr>
<tr>
<td>attacks</td>
<td></td>
</tr>
<tr>
<td>Global Rate-limit</td>
<td>Attack in which the global rate-limit threshold has been exceeded.</td>
</tr>
<tr>
<td>exceeded attacks</td>
<td></td>
</tr>
</tbody>
</table>

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 11-20 describes the fields in the `show statistics ddos global` command output.
Table 11-20  Field Descriptions for show ddos statistics global Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total packets received</td>
<td>Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.</td>
</tr>
<tr>
<td>Total packets dropped</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.</td>
</tr>
<tr>
<td>Total Anti-spoofing triggered</td>
<td>Total number of packets that triggered the GSS anti-spoofing mechanism.</td>
</tr>
<tr>
<td>Total Validated DNS requests</td>
<td>Total number of packets successfully identified as part of an anti-spoofing attack.</td>
</tr>
<tr>
<td>Rate-limit drops</td>
<td>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.</td>
</tr>
<tr>
<td>Global Rate-limit drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.</td>
</tr>
<tr>
<td>Unknown dproxies drops</td>
<td>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.</td>
</tr>
<tr>
<td>Spoofed packet drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an attack and dropped.</td>
</tr>
<tr>
<td>Malformed packet drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as a malformed packet and dropped.</td>
</tr>
<tr>
<td>Mitigation rules drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.</td>
</tr>
<tr>
<td>Global domain name drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.</td>
</tr>
<tr>
<td>Ongoing anti-spoofing drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.</td>
</tr>
</tbody>
</table>

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
```
Displaying DDoS Status

You display DDoS statistics by entering the `show ddos status` command (from privileged EXEC mode) or the `show status` command (from ddos configuration mode).

The syntax of this command is as follows:

```
show [ddos] status
```

Table 11-21 describes the field in the `show ddos status` command output.

### Table 11-21  Field Description for show [ddos] status Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Status</td>
<td>Status of the DDoS detection and mitigation module in the GSS, either enabled or disabled.</td>
</tr>
</tbody>
</table>

For example, enter:
```
gss1.yourdomain.com# show ddos status
DDoS Status: Disabled
```

Monitoring 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 view 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.

You use the `show statistics keepalive` command option to view 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 HTTPS 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 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 of this command is as follows:
Monitoring Global Server Load-Balancing Statistics from the CLI

Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

show statistics keepalive cra {ip_address | all | list}

The keywords and arguments are as follows:
- ip_address—IP address to display keepalive statistics. You can only use an IPv4 address.
- all—Displays all configured CRA-type keepalives.
- list—Lists all available IP addresses.

Table 11-22 describes the fields in the show statistics keepalive cra all command output.

Table 11-22  Field Descriptions for show statistics keepalive cra all Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>Name assigned to the answer.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and Suspended.</td>
</tr>
<tr>
<td>One Way Delay</td>
<td>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.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

Displaying Global Keepalive Statistics

You display all keepalive statistics managed by the GSS device by using the show statistics keepalive global command.

The syntax of this command is as follows:

show statistics keepalive global

Table 11-23 describes the fields in the show statistics keepalive global command output.

Table 11-23  Field Descriptions for show statistics keepalive global Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Probe Success Count</td>
<td>Number of ICMP queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>ICMP Probe Failure Count</td>
<td>Number of ICMP queries sent to the answer that resulted in a failure.</td>
</tr>
</tbody>
</table>
### Table 11-23  Field Descriptions for show statistics keepalive global Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP 'echo request' packets sent</td>
<td>Number of ICMP echo request messages sent to the answer.</td>
</tr>
<tr>
<td>ICMP 'echo reply' packets received</td>
<td>Number of ICMP echo reply messages received by the GSS from the answer.</td>
</tr>
<tr>
<td>Configured ICMP Probe Count</td>
<td>Number of configured ICMP probes sent to the answer.</td>
</tr>
<tr>
<td>ONLINE ICMP Probe Count</td>
<td>Number of ICMP probes sent to the answer that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>OFFLINE ICMP Probe Count</td>
<td>Number of ICMP probes sent to the answer that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED ICMP Probe Count</td>
<td>Number of ICMP probes sent to the answer that returned a Suspended state for the keepalive.</td>
</tr>
<tr>
<td>INIT ICMP Probe Count</td>
<td>Number of ICMP probes sent to the answer that returned an Init state for the keepalive.</td>
</tr>
<tr>
<td>DNS Probe Success Count</td>
<td>Number of DNS request probes sent by the GSS that resulted in a successful response.</td>
</tr>
<tr>
<td>DNS Probe Failure Count</td>
<td>Number of DNS request probes sent by the GSS that resulted in a failure.</td>
</tr>
<tr>
<td>DNS packets sent</td>
<td>Number of DNS request packets sent by the GSS.</td>
</tr>
<tr>
<td>DNS packets received</td>
<td>Number of DNS request packets received by the GSS.</td>
</tr>
<tr>
<td>Configured DNS Probe Count</td>
<td>Number of DNS request probes sent by the GSS.</td>
</tr>
<tr>
<td>ONLINE DNS Probe Count</td>
<td>Number of DNS request probes sent that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>OFFLINE DNS Probe Count</td>
<td>Number of DNS request probes that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED DNS Probe Count</td>
<td>Number of DNS request probes that returned a Suspended state for the keepalive.</td>
</tr>
<tr>
<td>INIT DNS Probe Count</td>
<td>Number of DNS request probes sent that returned an Init state for the keepalive.</td>
</tr>
<tr>
<td>KAL-AP Probe Success Count</td>
<td>Number of KAL-AP queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>KAL-AP Probe Failure Count</td>
<td>Number of KAL-AP queries sent to the answer that resulted in a failure.</td>
</tr>
<tr>
<td>KAL-AP packets sent</td>
<td>Number of KAL-AP packets sent to the answer.</td>
</tr>
<tr>
<td>KAL-AP packets received</td>
<td>Number of KAL-AP packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Configured KAL-AP Probe Count</td>
<td>Number of configured KAL-AP probes sent to the answer.</td>
</tr>
<tr>
<td>ONLINE KAL-AP Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>OFFLINE KAL-AP Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED KAL-AP Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive.</td>
</tr>
</tbody>
</table>
### Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

#### Monitoring Global Server Load-Balancing Statistics from the CLI

Table 11-23  **Field Descriptions for show statistics keepalive global Command (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INIT KAL-AP Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive.</td>
</tr>
<tr>
<td>CRA Probe Success Count</td>
<td>Number of CRA queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>CRA Probe Failure Count</td>
<td>Number of CRA queries sent to the answer that resulted in a failure.</td>
</tr>
<tr>
<td>CRA packets sent</td>
<td>Number of CRA packets sent to the answer.</td>
</tr>
<tr>
<td>CRA packets received</td>
<td>Number of CRA packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Configured CRA Probe Count</td>
<td>Number of configured CRA probes sent to the answer.</td>
</tr>
<tr>
<td>ONLINE CRA Probe Count</td>
<td>Number of CRA probes sent to the answer that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>OFFLINE CRA Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED CRA Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive.</td>
</tr>
<tr>
<td>INIT CRA Probe Count</td>
<td>Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive.</td>
</tr>
<tr>
<td>HTTP-HEAD Probe Success Count</td>
<td>Number of HTTP-HEAD queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>HTTPS-HEAD Probe Success Count</td>
<td>Number of HTTPS-HEAD queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>HTTPS-HEAD Probe Failure Count</td>
<td>Number of HTTPS-HEAD queries sent to the answer that resulted in a failure.</td>
</tr>
<tr>
<td>HTTPS-HEAD packets sent</td>
<td>Number of HTTPS-HEAD packets sent to the answer.</td>
</tr>
<tr>
<td>Configured HTTPS-HEAD Probe Count</td>
<td>Number of configured HTTPS-HEAD probes sent to the answer.</td>
</tr>
</tbody>
</table>
Table 11-23  Field Descriptions for show statistics keepalive global Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONLINE HTTPS-HEAD Probe Count</td>
<td>Number of configured HTTPS-HEAD probes sent to the answer.</td>
</tr>
<tr>
<td>OFFLINE HTTPS-HEAD Probe Count</td>
<td>Number of HTTPS-HEAD probes sent to the answer that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED HTTPS-HEAD Probe Count</td>
<td>Number of HTTPS-HEAD probes sent to the answer that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>INIT HTTPS-HEAD Probe Count</td>
<td>Number of HTTPS-HEAD probes sent to the answer that returned a Suspended state for the keepalive.</td>
</tr>
<tr>
<td>TCP Probe Success Count</td>
<td>Number of TCP queries sent to the answer that resulted in a successful response.</td>
</tr>
<tr>
<td>TCP Probe Failure Count</td>
<td>Number of TCP queries sent to the answer that resulted in a failure.</td>
</tr>
<tr>
<td>TCP packets sent</td>
<td>Number of TCP packets sent to the answer.</td>
</tr>
<tr>
<td>TCP packets received</td>
<td>Number of TCP packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Configured TCP Probe Count</td>
<td>Number of configured TCP probes sent to the answer.</td>
</tr>
<tr>
<td>ONLINE TCP Probe Count</td>
<td>Number of TCP probes sent to the answer that returned an Online state for the keepalive.</td>
</tr>
<tr>
<td>OFFLINE TCP Probe Count</td>
<td>Number of TCP probes sent to the answer that returned an Offline state for the keepalive.</td>
</tr>
<tr>
<td>SUSPENDED TCP Probe Count</td>
<td>Number of TCP probes sent to the answer that returned a Suspended state for the keepalive.</td>
</tr>
<tr>
<td>INIT TCP Probe Count</td>
<td>Number of TCP probes sent to the answer that returned an Init state for the keepalive.</td>
</tr>
<tr>
<td>Total Configured Probe Count</td>
<td>Total number of configured keepalive probes.</td>
</tr>
</tbody>
</table>

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 of this 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. Enter either an IPv4 or an IPv6 IP address.
- `all`—Displays all configured HTTP HEAD-type keepalives.
- `list`—Lists all available IP addresses.

Table 11-24 describes the fields in the `show statistics keepalive http-head all` command output.
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

You display statistics for configured HTTPS HEAD keepalive types managed by the GSS and used with VIP-type answers by using the `show statistics keepalive https-head` command.

The syntax of this command is as follows:

```
show statistics keepalive https-head {ip_address | all | list}
```

The keywords and arguments are as follows:

- `ip_address`—IP address to display keepalive statistics. Enter either an IPv4 or an IPv6 IP address.
- `all`—Displays all configured HTTP HEAD-type keepalives.
- `list`—Lists all available IP addresses.

`Table 11-25` describes the fields in the `show statistics keepalive https-head all` command output.

---

**Table 11-24 Field Descriptions for show statistics keepalive http-head all Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>IP address of the keepalive target.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and</td>
</tr>
<tr>
<td></td>
<td>Suspended.</td>
</tr>
<tr>
<td>Keepalive Type</td>
<td>Standard or Fast KAL-AP keepalive transmission rate used to define the</td>
</tr>
<tr>
<td></td>
<td>failure detection time for the GSS.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port on the remote device receiving the HTTP HEAD-type keepalive</td>
</tr>
<tr>
<td></td>
<td>request from the GSS.</td>
</tr>
<tr>
<td>HTTP Path</td>
<td>Default path that is relative to the server website being queried in the</td>
</tr>
<tr>
<td></td>
<td>HTTP HEAD request.</td>
</tr>
<tr>
<td>Host Tag</td>
<td>Domain name that is sent to the VIP as part of the HTTP HEAD query in the</td>
</tr>
<tr>
<td></td>
<td>Host tag field of the shared keepalive configuration.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online</td>
</tr>
<tr>
<td></td>
<td>state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

---

**Displaying HTTPS HEAD Keepalive Statistics**

You display statistics for configured HTTPS HEAD keepalive types managed by the GSS and used with VIP-type answers by using the `show statistics keepalive https-head` command.

The syntax of this command is as follows:

```
show statistics keepalive https-head {ip_address | all | list}
```

The keywords and arguments are as follows:

- `ip_address`—IP address to display keepalive statistics. Enter either an IPv4 or an IPv6 IP address.
- `all`—Displays all configured HTTP HEAD-type keepalives.
- `list`—Lists all available IP addresses.

`Table 11-25` describes the fields in the `show statistics keepalive https-head all` command output.
Chapter 11   Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

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 of this command is as follows:

```
show statistics keepalive icmp {ip_address | all | list}
```

The keywords and arguments are as follows:

- `ip_address`—Specifies the IP address to display keepalive statistics. You can use either an IPv4 or an IPv6 IP address.
- `all`—Displays all configured ICMP-type keepalives.
- `list`—Lists all available IP addresses.

Table 11-26 describes the fields in the `show statistics keepalive icmp all` command output.
Chapter 11    Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

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 of this 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. Enter an IPv4 IP address.
- `all`—Displays all configured KAL-AP-type keepalives.
- `list`—Lists all available IP addresses.

Table 11-27 describes the fields in the show statistics keepalive kalap all command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>IP address of the keepalive target.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and</td>
</tr>
<tr>
<td></td>
<td>Suspended.</td>
</tr>
<tr>
<td>Keepalive Type</td>
<td>Standard or Fast KAL-AP keepalive transmission rate used to define the</td>
</tr>
<tr>
<td></td>
<td>failure detection time for the GSS.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online</td>
</tr>
<tr>
<td></td>
<td>state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

Tag Alphanumeric tag associated with the VIP in the KAL-AP request.
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Table 11-27  Field Descriptions for show statistics keepalive kalap all Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Circuit</td>
<td>Primary (master) IP address.</td>
</tr>
<tr>
<td>Secondary Circuit</td>
<td>Secondary (backup) IP address.</td>
</tr>
<tr>
<td>Load</td>
<td>Load threshold value used to determine whether an answer is available, regardless of the balance method used.</td>
</tr>
<tr>
<td>Circuit Transitions</td>
<td>Number of times that the circuit changed state.</td>
</tr>
<tr>
<td>VIP Failovers</td>
<td>Number of times that the VIP switched to or from the primary DNS server and the secondary DNS server.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

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 of this command is as follows:

```
show statistics keepalive scripted-kal {name | all | list}
```

The keywords and arguments are as follows:

- `name`—KAL name for which you wish to display keepalive statistics.
- `all`—Displays all configured Scripted keepalives.
- `list`—Lists all available IP addresses.

Table 11-28 describes the fields in the show statistics keepalive scripted-kal all command output.

Table 11-28  Field Descriptions for show statistics keepalive scripted-kal all Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the SLB. Enter either an IPv4 or an IPv6 address.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>Target IP address of the keepalive.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and Suspended.</td>
</tr>
<tr>
<td>Keepalive Type</td>
<td>Type of keepalive. The potential types are CRA, ICMP, TCP, KAL-AP, Answer, Scripted keepalive, and HTTP-HEAD.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

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 of this 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. Enter an IPv4 address.

---

**Table 11-28  Field Descriptions for show statistics keepalive scripted-kal all Command (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kal Name</td>
<td>Name of the applicable keepalive.</td>
</tr>
<tr>
<td>Scripted Kal Type</td>
<td>Type of Scripted keepalive. The potential types are cisco-slb, f5-slb,</td>
</tr>
<tr>
<td>OID</td>
<td>SNMP request sent for this OID. There are two types of OIDs: scalar and</td>
</tr>
<tr>
<td></td>
<td>vector or table. For a scalar-type OID, the filter is not required, while</td>
</tr>
<tr>
<td></td>
<td>for a vector-type, it is a requirement.</td>
</tr>
<tr>
<td></td>
<td>When you query for the vector OID, you get all the information in the table</td>
</tr>
<tr>
<td></td>
<td>describing all of the VIPs configured at the target device. In this data,</td>
</tr>
<tr>
<td></td>
<td>the load information for some VIPs configured at the GSS is the only</td>
</tr>
<tr>
<td></td>
<td>information of real value, however.</td>
</tr>
<tr>
<td>OID Type</td>
<td>The OID-Type is supported for snmp-mib-indexed-by-vip and</td>
</tr>
<tr>
<td></td>
<td>snmp-mib-nonindexed-by-vip. There are two OID types: IpAddress or</td>
</tr>
<tr>
<td></td>
<td>InetAddress. The IpAddress setting is for compatibility purposes with an</td>
</tr>
<tr>
<td></td>
<td>older software release where the MIB structure supports the OID type as</td>
</tr>
<tr>
<td></td>
<td>IpAddress. If you specify InetAddress, the MIB structure supports the OID</td>
</tr>
<tr>
<td></td>
<td>type as InetAddress, and InetAddress supports IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td>Community Name</td>
<td>SNMP community name defined at the target device.</td>
</tr>
<tr>
<td>Filter</td>
<td>Required entry when fetching load information for some VIPs configured at</td>
</tr>
<tr>
<td></td>
<td>the GSS.</td>
</tr>
<tr>
<td>Load</td>
<td>Load threshold value used to determine whether an answer is available,</td>
</tr>
<tr>
<td></td>
<td>regardless of the balance method used.</td>
</tr>
<tr>
<td>Max VIP Load</td>
<td>Value that the user sets at the Answer page.</td>
</tr>
<tr>
<td>No. of Execution</td>
<td>Number of times that the script is executed.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a</td>
</tr>
<tr>
<td></td>
<td>negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online</td>
</tr>
<tr>
<td></td>
<td>state) experienced by the keepalive.</td>
</tr>
<tr>
<td>VIP GID</td>
<td>VIP Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
<tr>
<td>Keepalive GID</td>
<td>Global ID number of the keepalive.</td>
</tr>
</tbody>
</table>
• **all**—Displays all configured name server-type keepalives.
• **list**—Lists all available IP addresses.

Table 11-29 describes the fields in the `show statistics keepalive ns all` command output.

**Table 11-29  Field Descriptions for show statistics keepalive ns all Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>IP address of the keepalive target.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and Suspended.</td>
</tr>
<tr>
<td>Domain</td>
<td>Globally defined domain name that the GSS queries when utilizing the NS keepalive.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

### 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 of this 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. Enter an IPv4 or an IPv6 IP address.
- **all**—Displays all configured TCP-type keepalives.
- **list**—Lists all available IP addresses.

Table 11-30 describes the fields in the `show statistics keepalive tcp all` command output.

**Table 11-30  Field Descriptions for show statistics keepalive tcp all Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>IP address of the keepalive target.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

The proximity component displays statistics about the network proximity operation 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 of this command is as follows:

```
show statistics dns proximity rule
```

Table 11-31 describes the fields in the `show statistics dns proximity rule` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>State of the keepalive. The possible states are Online, Offline, Init, and Suspended.</td>
</tr>
<tr>
<td>Keepalive Type</td>
<td>Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Port on the remote device receiving the TCP keepalive request.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Total number of keepalive packets sent to the answer by the GSS.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Total number of keepalive packets received by the GSS from the answer.</td>
</tr>
<tr>
<td>Positive Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.</td>
</tr>
<tr>
<td>Negative Probe</td>
<td>Total number of keepalive probes sent to the answer that resulted in a negative response.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.</td>
</tr>
<tr>
<td>GID</td>
<td>Global ID number used by the GSS.</td>
</tr>
<tr>
<td>LID</td>
<td>Local ID number used by the GSS.</td>
</tr>
</tbody>
</table>

Monitoring Network Proximity Statistics on a GSS

You display all proximity lookups by DNS rule name by using the `show statistics dns proximity rule` command.

The syntax of this command is as follows:

```
show statistics dns proximity rule
```

Table 11-31 describes the fields in the `show statistics dns proximity rule` command output.
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

### Displaying Proximity Database Statistics

You can view overall statistics on the proximity database, such as the number of entries currently in the proximity database, the number of entries dropped, and the rate of lookups by using the `show statistics proximity database` command.

The syntax of this command is as follows:

```plaintext
show statistics proximity database
```

Table 11-32 describes the fields in the `show statistics proximity database` command output.

#### Table 11-32  Field Descriptions for show statistics proximity database Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Entries in Use</td>
<td>Number of entries currently in the proximity database.</td>
</tr>
<tr>
<td>Number of Add Entries Dropped</td>
<td>Number of entry creation requests that the GSS dropped because the proximity database limit had been reached.</td>
</tr>
<tr>
<td>Max Number of Entries Used</td>
<td>Maximum number of entries used in the proximity database.</td>
</tr>
<tr>
<td>Max Number of Entries Allowed</td>
<td>Maximum number of entries that the proximity database can hold (500,000 entries).</td>
</tr>
<tr>
<td>Number of Database Dump Started</td>
<td>Number of times the GSS initiated a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps</td>
</tr>
<tr>
<td>Number of Database Dump Completed</td>
<td>Number of times the GSS completed a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps</td>
</tr>
<tr>
<td>Number of Database Dump Failed</td>
<td>Number of times the GSS failed to perform a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps</td>
</tr>
<tr>
<td>Last Database Dump Started Time</td>
<td>The last time the GSS started a proximity database dump.</td>
</tr>
<tr>
<td>Last Database Dump Failed Time</td>
<td>The last time the GSS failed to complete a proximity database dump.</td>
</tr>
<tr>
<td>Number of Database Cleanup Started</td>
<td>Number of times the GSS initiated a database cleanup to remove the least recently used entries from the proximity database.</td>
</tr>
<tr>
<td>Number of Database Cleanup Completed</td>
<td>Number of times the GSS completed a database cleanup to remove the least recently used entries from the proximity database.</td>
</tr>
</tbody>
</table>
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 of this command is as follows:

```plaintext
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 11-33 describes the fields in the `show statistics proximity group-summary` command output.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Unique alphanumeric name of the proximity group.</td>
</tr>
<tr>
<td>Target IP</td>
<td>Probe target IP address used by the proximity group, displayed in dotted-decimal notation.</td>
</tr>
<tr>
<td>Total Entries</td>
<td>Total number of D-proxy IP address and subnet mask pairs contained in the proximity group.</td>
</tr>
<tr>
<td>Total Hits</td>
<td>Accumulated hit count for all entries in the proximity group. Increments when a match occurs for any proximity group entry in the group.</td>
</tr>
</tbody>
</table>

You display statistics for a specific proximity group by using the `show statistics proximity group-name` command.

The syntax of this command is as follows:

```plaintext
show statistics proximity group-name groupname
```

Enter the exact name of a proximity group to display all proximity database entries related to that group. Table 11-34 describes the fields in the `show statistics proximity group-name` command output.
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 of this command is as follows:

```
show statistics proximity lookup
```

Table 11-35 describes the fields in the `show statistics proximity lookup` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total lookup requests</td>
<td>Total number of proximity lookup requests made to the proximity database.</td>
</tr>
<tr>
<td>Database entry not found</td>
<td>Number of times the GSS was unable to locate a proximate answer in the database.</td>
</tr>
<tr>
<td>Partial RTT data returned</td>
<td>Number of times only partial round-trip time (RTT) data was returned to the DNS service by the proximity subsystem.</td>
</tr>
<tr>
<td>Current lookup request rate</td>
<td>Current request rate per second that requests are made by the DNS service to perform a proximity lookup in the database.</td>
</tr>
<tr>
<td>Peak lookup request rate</td>
<td>Peak request rate per second that requests are made by the DNS service to perform a proximity lookup in the database.</td>
</tr>
<tr>
<td>Lookup failed due to database full</td>
<td>Number of times the GSS was unable to complete a proximity lookup because the database exceeded the maximum number of entries.</td>
</tr>
<tr>
<td>Last database full happened</td>
<td>Last time the proximity database was full.</td>
</tr>
</tbody>
</table>

Displaying Proximity Probe Transfer Statistics

You display general probe success and failure counts by using the `show statistics proximity probes` command.

The syntax of this command is as follows:

```
show statistics proximity probes
```
show statistics proximity probes

Table 11-36 describes the fields in the **show statistics proximity probes** command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Whether the GSS performs DRP authentication when exchanging packets with the DRP agent in a proximity probing agent. States are Enabled and Disabled.</td>
</tr>
<tr>
<td>Echo Rx</td>
<td>Number of DRP echo responses received by the GSS from all configured proximity probing agents.</td>
</tr>
<tr>
<td>Echo Tx</td>
<td>Number of DRP echo requests sent by the GSS to all configured proximity probing agents.</td>
</tr>
<tr>
<td>Measure Rx</td>
<td>Number of DRP measured requests received by the GSS from all configured proximity probing agents.</td>
</tr>
<tr>
<td>Measure Tx</td>
<td>Number of DRP measured requests sent by the GSS to all configured proximity probing agents.</td>
</tr>
<tr>
<td>Pkts Rx</td>
<td>Total number of DRP packets received by the GSS from all configured proximity probing agents.</td>
</tr>
<tr>
<td>Pkts Tx</td>
<td>Number of DRP packets sent by the GSS to all configured proximity probing agents.</td>
</tr>
</tbody>
</table>

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 proximity probing agents (ONLINE or OFFLINE).

The syntax of this command is as follows:

```
show statistics proximity probes detailed
```

Table 11-37 describes the fields in the **show statistics proximity probes detailed** command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone ID</td>
<td>Numerical identifier of the proximity zone.</td>
</tr>
<tr>
<td>Zone Name</td>
<td>Name of the proximity zone.</td>
</tr>
<tr>
<td>Authentication</td>
<td>An indication of whether the GSS performs DRP authentication when exchanging packets with the DRP agent in a proximity probing agent.</td>
</tr>
<tr>
<td>Primary</td>
<td>Identifies the IP address of the primary proximity probing agent servicing this zone and the status of the proximity probing agent (ONLINE or OFFLINE).</td>
</tr>
<tr>
<td>Secondary</td>
<td>Identifies the IP address of the backup proximity probing agent servicing this zone and the status of the proximity probing agent (ONLINE or OFFLINE).</td>
</tr>
<tr>
<td>Echo Rx</td>
<td>Number of DRP echo responses received by the GSS from all configured proximity probing agents.</td>
</tr>
<tr>
<td>Echo Tx</td>
<td>Number of DRP echo requests sent by the GSS to all configured proximity probing agents.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

Displaying Proximity Status

You display general status information about the proximity subsystem by using the `show proximity` command.

The syntax of this command is as follows:

```
show proximity
```

Table 11-38 describes the fields in the `show proximity` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proximity subsystem status</td>
<td>Current operating status of the Proximity subsystem component.</td>
</tr>
<tr>
<td>Proximity database dump interval</td>
<td>Time period between automatic proximity database dumps performed by the GSS.</td>
</tr>
<tr>
<td>Proximity database age-out interval</td>
<td>Time period between checks by the GSS to verify when the user-configured entry inactivity timeout value elapses.</td>
</tr>
</tbody>
</table>

Displaying Proximity Group Configuration

You display a summary of all configured proximity groups by using the `show proximity group-summary` command.

```
show proximity group-summary
```

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 11-39 describes the fields in the `show proximity group-summary` command output.
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

You display the configuration of a specific proximity group by using the `show proximity group-name` command.

The syntax of this command is as follows:

```
show proximity group-name groupname
```

Enter the exact name of a proximity group to display all proximity entries related to that group.

Table 11-39 describes the fields in the `show proximity group-name` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique alphanumeric name of the proximity group</td>
</tr>
<tr>
<td>Address Blocks</td>
<td>IP address block of the proximity group, specified in dotted-decimal notation</td>
</tr>
</tbody>
</table>

Displaying Proximity Database Status

You display the proximity database (PDB) entries by specifying one or more entry matching criteria by entering 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 as follows:

- **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 (IPv4 or IPv6) address of the requesting client’s D-proxy. Enter IPv4 address in dotted-decimal notation or for an IPv6 address, use a double, no double colon, and a slash followed by a number (/n) notation. The prefix-length range for IPv4 address is from 1 to 31 and for IPv6 addresses, the range is from 1 to 127. For example, 192.168.11.1 or 2001:DB8::A:B:1.
- **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 all
```
### Monitoring 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 the 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 of this command is as follows:

```
show statistics dns sticky rule
```

Table 11-41 describes the fields in the `show statistics dns sticky rule` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Name of the matched DNS rule.</td>
</tr>
<tr>
<td>Hits</td>
<td>Total number of successful lookups in the sticky database for the sticky database entry.</td>
</tr>
<tr>
<td>Misses</td>
<td>Total number of failed lookups in the sticky database for the DNS rule.</td>
</tr>
<tr>
<td>Additions</td>
<td>Total number of times that a request matched on a DNS rule, resulting in the GSS adding an entry to the sticky database.</td>
</tr>
</tbody>
</table>
Displaying Sticky Statistics

You display general statistics about the sticky database, 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 by using the `show statistics sticky` command.

The syntax of this command is as follows:

```
show statistics sticky
```

Table 11-42 describes the fields in the `show statistics sticky` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current entry count</td>
<td>Current number of entries in the sticky database.</td>
</tr>
<tr>
<td>Highest entry count</td>
<td>Maximum number of entries in the sticky database since the last time sticky was enabled or the sticky statistics were cleared.</td>
</tr>
<tr>
<td>Total Lookups</td>
<td>Total number of lookups in the sticky database.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of successful lookups in the sticky database.</td>
</tr>
<tr>
<td>Misses</td>
<td>Number of failed lookups in the sticky database.</td>
</tr>
<tr>
<td>Addition success</td>
<td>Number of addition requests for the sticky database that succeeded.</td>
</tr>
<tr>
<td>Addition fail</td>
<td>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.</td>
</tr>
<tr>
<td>Modification success</td>
<td>Number of answer modification requests that succeeded.</td>
</tr>
<tr>
<td>Modification fail</td>
<td>Number of answer modification requests that failed.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>Number of entries removed from the sticky database because the answer exceeded the user-configured Entry Inactivity Timeout value.</td>
</tr>
<tr>
<td>Reclaimed</td>
<td>Number of entries removed from the sticky database due to an overflow.</td>
</tr>
<tr>
<td>CLI deletions local</td>
<td>Number of entries manually deleted from the sticky database through the sticky database delete CLI command, entered on the local GSS node.</td>
</tr>
<tr>
<td>CLI deletions remote</td>
<td>Number of entries manually deleted from the sticky database through the sticky database delete CLI command, entered on a GSS peer.</td>
</tr>
</tbody>
</table>

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 of this 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 11-43 describes the fields in the `show statistics sticky global` command output.
### Table 11-43  
**Field Descriptions for show statistics sticky global Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Type</td>
<td>Statistics on sticky database entry operations performed by the local GSS node.</td>
</tr>
<tr>
<td>Send OK</td>
<td>Sticky database entry messages transmitted by the local GSS node without a failure.</td>
</tr>
<tr>
<td>Send Fail</td>
<td>Sticky database entry messages transmitted by the local GSS node with errors.</td>
</tr>
<tr>
<td>Received</td>
<td>Sticky database entry messages received by the local GSS node from GSS peers.</td>
</tr>
<tr>
<td>Add</td>
<td>Number of new entries added to the sticky database of the local GSS node.</td>
</tr>
<tr>
<td>Modify</td>
<td>Number of sticky database entries modified by the local GSS node due to a keepalive failure.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>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.</td>
</tr>
<tr>
<td>Lookup Slow</td>
<td>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.</td>
</tr>
<tr>
<td>Remove</td>
<td>Number of entries removed from the sticky database of the local GSS node through the <strong>sticky database delete</strong> command. Entries removed by the <strong>sticky database delete all</strong> command are reflected in the Remove All field (see the description that follows).</td>
</tr>
<tr>
<td>Add Sync</td>
<td>Number of entries added to the sticky database of the local GSS node due to the result of a peer synchronization, and not to a normal DNS client request.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Statistics on sticky database messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Send OK</td>
<td>Messages transmitted by the local GSS node without a failure.</td>
</tr>
<tr>
<td>Send Fail</td>
<td>Messages transmitted by the local GSS node with errors.</td>
</tr>
<tr>
<td>Received</td>
<td>Messages received by the local GSS node from GSS peers.</td>
</tr>
<tr>
<td>Add</td>
<td>Number of Add entry type messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Modify</td>
<td>Number of Modify entry type messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>Number of Lookup Fast entry type messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Lookup Slow</td>
<td>Number of Lookup Slow entry type messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Remove</td>
<td>Number of Remove messages sent or received by the local GSS node.</td>
</tr>
</tbody>
</table>
### Table 11-43 Field Descriptions for show statistics sticky global Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Sync</td>
<td>Number of Add Sync entry type messages sent or received by the local GSS node.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Number of times the <strong>sticky database delete all</strong> 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.</td>
</tr>
<tr>
<td>Request Db</td>
<td>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.</td>
</tr>
<tr>
<td>Ack RequestDb</td>
<td>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.</td>
</tr>
<tr>
<td>Refuse Db Req</td>
<td>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.</td>
</tr>
<tr>
<td>Sync Start</td>
<td>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 <strong>sticky database delete</strong> 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.</td>
</tr>
<tr>
<td>Sync Done</td>
<td>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 <strong>sticky database delete</strong> command) while any GSS within the mesh is performing a synchronization.</td>
</tr>
<tr>
<td>Version mis-match</td>
<td>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.</td>
</tr>
</tbody>
</table>
Monitoring Global Server Load-Balancing Statistics from the CLI

**Table 11-43  Field Descriptions for show statistics sticky global Command (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock Out Of Sync</td>
<td>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 greater than 3 minutes with the other GSS peers ignores update messages from all peers until you resynchronize its system clock (see Chapter 9, Configuring DNS Sticky, for details).</td>
</tr>
</tbody>
</table>

| Mask mis-match               | Error message indicating the number of times 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. 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 9, Configuring DNS Sticky, for details). |

**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 11-44 describes the fields in the `show statistics sticky mesh` command output.

**Table 11-44  Field Descriptions for show statistics sticky mesh Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Information for application sticky</td>
<td>Status and statistics about the global sticky mesh.</td>
</tr>
<tr>
<td>Transmit Pkts</td>
<td>Total number of application data packets transmitted by the local GSS node to GSS peers in the mesh.</td>
</tr>
<tr>
<td>Transmit Bytes</td>
<td>Total number of application data bytes transmitted by the local GSS node to GSS peers in the mesh.</td>
</tr>
<tr>
<td>Receive Pkts</td>
<td>Total number of application data packets received by the local GSS node from GSS peers in the mesh.</td>
</tr>
<tr>
<td>Receive Bytes</td>
<td>Total number of application data bytes received by the local GSS node from GSS peers in the mesh.</td>
</tr>
<tr>
<td>Dropped Tx Pkts</td>
<td>Total number of packets to be transmitted by the local GSS node but were dropped due to buffer errors.</td>
</tr>
<tr>
<td>Dropped Rx Pkts</td>
<td>Total number of packets received by the local GSS node but were dropped due to buffer errors.</td>
</tr>
<tr>
<td>Current TxQueue</td>
<td>Total number of packets in the buffer transmit queue of the local GSS node that are waiting to be transmitted.</td>
</tr>
<tr>
<td>Maximum TxQueue</td>
<td>Maximum number of packets that have been in the buffer transmit queue of the local GSS node.</td>
</tr>
</tbody>
</table>
### Table 11-44  Field Descriptions for show statistics sticky mesh Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current RxQueue</td>
<td>Total number of packets in the buffer receive queue of the local GSS node that are waiting to be received.</td>
</tr>
<tr>
<td>Maximum RxQueue</td>
<td>Maximum number of packets that have been in the buffer receive queue of the local GSS node.</td>
</tr>
<tr>
<td>Buffers Alloc’d</td>
<td>Number of optimal-sized frames allocated for the buffer transmit and buffer receive data.</td>
</tr>
<tr>
<td>Buffers Free</td>
<td>Number of buffers currently free in the local GSS node.</td>
</tr>
<tr>
<td>Session Information for GSS peer</td>
<td>Status and statistics for a specific GSS peer in the mesh.</td>
</tr>
<tr>
<td>GSS ID</td>
<td>Unique identifier of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>CurTx Data Pkts</td>
<td>Number of data packets sent by the local GSS node to the GSS peer during the current session.</td>
</tr>
<tr>
<td>CurTx Data Bytes</td>
<td>Number of data bytes sent by the local GSS node to the GSS peer during the current session.</td>
</tr>
<tr>
<td>TtlTx Data Pkts</td>
<td>Number of application data packets sent by the local GSS node to the GSS peer for the total duration of the mesh.</td>
</tr>
<tr>
<td>TtlTx Data Bytes</td>
<td>Number of application data bytes sent by the local GSS node to the GSS peer for the total duration of the mesh.</td>
</tr>
<tr>
<td>Transmit Pkts</td>
<td>Total number of packets transmitted from the local GSS node to the GSS peer (including application packets, control packets, RTT packets, and keepalive packets).</td>
</tr>
<tr>
<td>Transmit Bytes</td>
<td>Total number of bytes transmitted from the local GSS node to the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes).</td>
</tr>
<tr>
<td>CurRx Data Pkts</td>
<td>Number of data packets received by the local GSS node from the GSS peer during the current session.</td>
</tr>
<tr>
<td>CurRx Data Bytes</td>
<td>Number of data bytes received by the local GSS node from the GSS peer during the current session.</td>
</tr>
<tr>
<td>TtlRx Data Pkts</td>
<td>Number of application data packets received by the local GSS node from the GSS peer for the total duration of the mesh.</td>
</tr>
<tr>
<td>TtlRx Data Bytes</td>
<td>Number of application data bytes received by the local GSS node from the GSS peer for the total duration of the mesh.</td>
</tr>
<tr>
<td>Receive Pkts</td>
<td>Total number of packets received by the local GSS node from the GSS peer (including application packets, control packets, RTT packets, and keepalive packets).</td>
</tr>
<tr>
<td>Receive Bytes</td>
<td>Total number of bytes received by the local GSS node from the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes).</td>
</tr>
<tr>
<td>ConnectFailures</td>
<td>Number of times that the connection attempt failed between the local GSS node and the GSS peer.</td>
</tr>
<tr>
<td>CurConnAttempts</td>
<td>Number of current connection attempts between the local GSS node and the GSS peer.</td>
</tr>
</tbody>
</table>
Monitoring Global Server Load-Balancing Statistics from the CLI

Chapter 11 Monitoring GSS Global Server Load-Balancing Operation

### 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 11-45 describes the fields in the `show statistics sticky group-summary` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Unique alphanumeric name of the DNS sticky group.</td>
</tr>
<tr>
<td>Group Number</td>
<td>IP address block of the sticky group, specified in dotted-decimal notation.</td>
</tr>
<tr>
<td>Total Entries</td>
<td>Total number of D-proxy IP address and subnet mask pairs contained in the sticky group.</td>
</tr>
<tr>
<td>Total Hits</td>
<td>Accumulated hit count for all entries in the sticky group. Increments when a match occurs for each sticky group entry.</td>
</tr>
</tbody>
</table>

You display statistics for a specific sticky group by using the `show statistics sticky group-name` command.

The syntax of this command is as follows:

```
show statistics sticky group-name {groupname}
```

Enter the exact name of a sticky group to display all sticky entries related to that group.

Table 11-46 describes the fields in the `show statistics sticky group-name` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Unique alphanumeric name of the DNS sticky group.</td>
</tr>
<tr>
<td>Group Number</td>
<td>IP address block of the sticky group, specified in dotted-decimal notation.</td>
</tr>
<tr>
<td>Total Entries for Group</td>
<td>Total number of D-proxy IP addresses included in the sticky group.</td>
</tr>
<tr>
<td>Address</td>
<td>D-proxy IP address included in the sticky group.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Subnet mask included in the sticky group, displayed as an integer (for example, 24 or 32).</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number that increments when a match occurs for this sticky group entry.</td>
</tr>
<tr>
<td>Last Time Hit</td>
<td>Last time the hit count incremented due to an entry match.</td>
</tr>
</tbody>
</table>
Displaying the Sticky Status

You display general status information about the sticky subsystem by using the `show sticky` command. The syntax of this command is as follows:

```
show sticky
```

Table 11-47 describes the fields in the `show sticky` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sticky Manager status</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Initializing—Appears only during boot time or after entering the <code>gss start</code> CLI command.</td>
</tr>
<tr>
<td></td>
<td>• Disabled via GUI—Appears after you disable sticky from the primary GSSM GUI.</td>
</tr>
<tr>
<td></td>
<td>• Stopped via CLI—Appears after you enter the <code>sticky stop</code> CLI command.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Database entry count</td>
<td>Current number of entries in the sticky database.</td>
</tr>
<tr>
<td>Dump status</td>
<td>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.</td>
</tr>
<tr>
<td>Dump interval</td>
<td>Time period between automatic sticky database dumps performed by the GSS.</td>
</tr>
<tr>
<td>Reclaim status</td>
<td>Current operating status of the overflow recovery subsystem. The Reclaim status messages include Initialized, Disabled, Waiting, and In Progress.</td>
</tr>
<tr>
<td>Timeout status</td>
<td>Current operating status of the entry inactivity timeout subsystem. The Timeout status messages include Initialized, Disabled, Waiting, and In Progress.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Table 11-47  Field Descriptions for show sticky Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout interval</td>
<td>Time period between checks by the GSS to verify when the user-configured sticky inactivity timeout value elapses.</td>
</tr>
<tr>
<td>Mesh status</td>
<td>Current operating status of the sticky global mesh. Status messages are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Running—The GSS is operating properly in the sticky mesh.</td>
</tr>
<tr>
<td></td>
<td>• Failed—The GSS is unable to operate properly in the sticky mesh.</td>
</tr>
<tr>
<td></td>
<td>• Waiting—The GSS is waiting for mesh configuration information.</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Global sticky is enabled on the local GSS node.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Global sticky is disabled on the local GSS node (either from the primary GSSM GUI or through the sticky stop CLI command).</td>
</tr>
</tbody>
</table>

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 of this 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 as follows:

- **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 rule_name**—Displays all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

Table 11-48 describes the fields in the show sticky database all command output.
The following example displays the output of `show sticky database` command:

```
gss1.example.com# show sticky database region 117
Displayed 1 database entry.
gssm1.cisco.com#
```

### 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.

To view a more detailed listing of recent global sticky message identifiers, specify the `verbose` keyword. The syntax of this command is as follows:

```
show sticky global [verbose]
```

Table 11-49 describes the fields in the `show sticky global` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Peer Count</td>
<td>Total number of GSS peers in a sticky mesh (not including the local GSS node).</td>
</tr>
<tr>
<td>Last Message ID Sent for Each Message Type</td>
<td>Summary of the unique global sticky message identifiers last sent by the local GSS node.</td>
</tr>
<tr>
<td>Add</td>
<td>Unique identifier of the last Add entry-type message sent by the local GSS node.</td>
</tr>
</tbody>
</table>
Table 11-49  **Field Descriptions for show sticky global Command (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify</td>
<td>Unique identifier of the last Modify entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Details of Most Recently Received Messages by Peer</td>
<td>Status summary of the global sticky message identifiers last received by the local GSS node.</td>
</tr>
<tr>
<td>Peer Name</td>
<td>Hostname of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>Unique identifier of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Last Type</td>
<td>Type of the message last received from the peer.</td>
</tr>
<tr>
<td>Last Status</td>
<td>Status of the last message received from the peer.</td>
</tr>
<tr>
<td>Last MessageID Received for each Message Type...</td>
<td>Summary of the unique global sticky messages last received by the local GSS node from each GSS mesh peer.</td>
</tr>
<tr>
<td>Add</td>
<td>Unique identifier of the last Add entry-type message received by the local GSS node from the GSS peer.</td>
</tr>
<tr>
<td>Modify</td>
<td>Unique identifier of the last Modify entry-type message received by the local GSS node from the GSS peer.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>Unique identifier of the last Lookup Fast entry-type message received by the local GSS node from the GSS peer.</td>
</tr>
</tbody>
</table>

Table 11-50 describes the fields in the `show sticky global verbose` command output.
### Table 11-50  Field Descriptions for show sticky global verbose Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Peer Count</td>
<td>Total number of GSS peers in a sticky mesh (not including the local GSS node).</td>
</tr>
<tr>
<td>Last Message ID Sent for Each Message Type</td>
<td>Summary of the unique global sticky message identifiers last sent by the local GSS node.</td>
</tr>
<tr>
<td>Add</td>
<td>Unique identifier of the last Add entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Modify</td>
<td>Unique identifier of the last Modify entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Lookup Slow</td>
<td>Unique identifier of the last Lookup Slow entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Remove</td>
<td>Unique identifier of the last Remove entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Add Sync</td>
<td>Unique identifier of the last Add Sync entry-type message sent by the local GSS node.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Unique identifier of the last Remove All message sent by the local GSS node.</td>
</tr>
<tr>
<td>Request Db</td>
<td>Unique identifier of the last Request Db message sent by the local GSS node.</td>
</tr>
<tr>
<td>Ack ReqDb</td>
<td>Unique identifier of the last Ack ReqDb message sent by the local GSS node.</td>
</tr>
<tr>
<td>Refuse ReqDb</td>
<td>Unique identifier of the last Refuse ReqDb message sent by the local GSS node.</td>
</tr>
<tr>
<td>Sync Start</td>
<td>Unique identifier of the last Sync Start message sent by the local GSS node.</td>
</tr>
<tr>
<td>Sync Done</td>
<td>Unique identifier of the last Sync Done message sent by the local GSS node.</td>
</tr>
<tr>
<td>Details of Most Recently Received Messages by Peer</td>
<td>Status summary of the global sticky message identifiers last received by the local GSS node.</td>
</tr>
<tr>
<td>Peer Name</td>
<td>Hostname of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>Unique identifier of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Last Type</td>
<td>Type of the message last received from the peer.</td>
</tr>
</tbody>
</table>
Table 11-50  Field Descriptions for show sticky global verbose Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Status</td>
<td>Status of the last message received from the peer. Status messages are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Received OK—Message was received and processed.</td>
</tr>
<tr>
<td></td>
<td>• Version mismatch—Message dropped because the local GSS node was unable to communicate with</td>
</tr>
<tr>
<td></td>
<td>a peer due to different versions of the GSS software.</td>
</tr>
<tr>
<td></td>
<td>• Clock out of sync—Local GSS node was unable to communicate with a peer due to clock</td>
</tr>
<tr>
<td></td>
<td>synchronization issues. A GSS that has a system clock that is out of synchronization by</td>
</tr>
<tr>
<td></td>
<td>more than three minutes with the other GSS peers ignores update messages from all peers until</td>
</tr>
<tr>
<td></td>
<td>you resynchronize its system clock (see Chapter 9, Configuring DNS Sticky, for details).</td>
</tr>
<tr>
<td></td>
<td>• Mask mismatch—Local GSS node was unable to communicate with a peer due to a difference in</td>
</tr>
<tr>
<td></td>
<td>global subnet mask values. A GSS will drop all global sticky messages received from a GSS</td>
</tr>
<tr>
<td></td>
<td>with a different subnet mask. A difference in global sticky masks on a peer would occur only</td>
</tr>
<tr>
<td></td>
<td>if a configuration change was made on the primary GSSM GUI and the peer did not receive the</td>
</tr>
<tr>
<td></td>
<td>change due to a network failure. See Chapter 9, Configuring DNS Sticky, for details about</td>
</tr>
<tr>
<td></td>
<td>globally configuring the subnet mask of all GSS devices in the mesh from the primary GSSM</td>
</tr>
<tr>
<td></td>
<td>GUI.</td>
</tr>
<tr>
<td>Last MessageID</td>
<td>Summary of the unique global sticky messages last received by the local GSS node from each</td>
</tr>
<tr>
<td>Received for each</td>
<td>GSS mesh peer.</td>
</tr>
<tr>
<td>Message Type...</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Unique identifier of the last Add entry-type message received by the local GSS node from the</td>
</tr>
<tr>
<td></td>
<td>GSS peer.</td>
</tr>
<tr>
<td>Modify</td>
<td>Unique identifier of the last Modify entry-type message received by the local GSS node from</td>
</tr>
<tr>
<td></td>
<td>the GSS peer.</td>
</tr>
<tr>
<td>Lookup Fast</td>
<td>Unique identifier of the last Lookup Fast entry-type message received by the local GSS node</td>
</tr>
<tr>
<td></td>
<td>from the GSS peer.</td>
</tr>
<tr>
<td>Lookup Slow</td>
<td>Unique identifier of the last Lookup Slow entry-type message received by the local GSS node</td>
</tr>
<tr>
<td></td>
<td>from the GSS peer.</td>
</tr>
<tr>
<td>Remove</td>
<td>Unique identifier of the last Remove entry-type message received by the local GSS node from</td>
</tr>
<tr>
<td></td>
<td>the GSS peer.</td>
</tr>
<tr>
<td>Add Sync</td>
<td>Unique identifier of the last Add Sync entry-type message received by the local GSS node from</td>
</tr>
<tr>
<td></td>
<td>the GSS peer.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Unique identifier of the last Remove All message received by the local GSS node from the GSS</td>
</tr>
<tr>
<td></td>
<td>peer.</td>
</tr>
<tr>
<td>Request Db</td>
<td>Unique identifier of the last Request Db message received by the local GSS node from the GSS</td>
</tr>
<tr>
<td></td>
<td>peer.</td>
</tr>
<tr>
<td>Ack ReqDb</td>
<td>Unique identifier of the last Ack ReqDb message received by the local GSS node from the GSS</td>
</tr>
<tr>
<td></td>
<td>peer.</td>
</tr>
<tr>
<td>Refuse Db</td>
<td>Unique identifier of the last Refuse ReqDb message received by the local GSS node from the GSS</td>
</tr>
<tr>
<td></td>
<td>peer.</td>
</tr>
</tbody>
</table>
Monitoring Global Server Load-Balancing Statistics from the CLI

Displaying the 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 and options for this command are 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 11-51 describes the fields in the `show sticky mesh` command output.

### Table 11-50 Field Descriptions for show sticky global verbose Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Start</td>
<td>Unique identifier of the last Sync Start message received by the local GSS node from the GSS peer.</td>
</tr>
<tr>
<td>Sync Done</td>
<td>Unique identifier of the last Sync Done message received by the local GSS node from the GSS peer.</td>
</tr>
</tbody>
</table>

### Table 11-51 Field Descriptions for show sticky mesh Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My GSS ID</td>
<td>Unique identifier of the local GSS node in the mesh.</td>
</tr>
<tr>
<td>Mesh ID</td>
<td>Unique identifier of the global sticky mesh.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user-configurable.</td>
</tr>
<tr>
<td>Remote GSS IP Address/Host Name</td>
<td>IP address or hostname of the GSS peer in the mesh.</td>
</tr>
</tbody>
</table>
Chapter 11    Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Server Load-Balancing Statistics from the CLI

Table 11-51  Field Descriptions for show sticky mesh Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.</td>
</tr>
</tbody>
</table>
| State | State of the communication link between the local GSS node and the mesh peer. The possible states are as follows:  
  • 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. |

Table 11-52 describes the fields in the show sticky mesh session command output.

Table 11-52  Field Descriptions for show sticky mesh session Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Information for GSS peer</td>
<td>Hostname of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.</td>
</tr>
<tr>
<td>RTT</td>
<td>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.</td>
</tr>
</tbody>
</table>
| State | State of the communication link between the local GSS node and the mesh peer. The possible states are as follows:  
  • 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 11-53 describes the fields in the show sticky mesh session verbose command output.
### Table 11-53  Field Descriptions for `show sticky mesh session verbose` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Information for GSS peer</td>
<td>Identifies the host name of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.</td>
</tr>
<tr>
<td>Session State</td>
<td>State of the communication link between the local GSS node and the mesh peer. The possible states are as follows:</td>
</tr>
<tr>
<td></td>
<td>• SESSION_STOP—Indicates that the session is dead.</td>
</tr>
<tr>
<td></td>
<td>• SESSION_INIT—Indicates that the session is initializing.</td>
</tr>
<tr>
<td></td>
<td>• SESSION_OPEN—Indicates that the connection to the peer has been made.</td>
</tr>
<tr>
<td></td>
<td>• SESSION_AUTH—Indicates that authentication is occurring.</td>
</tr>
<tr>
<td></td>
<td>• SESSION_UP—Indicates that the session is up.</td>
</tr>
<tr>
<td></td>
<td>• SESSION_DOWN—Indicates that the session is down or failing.</td>
</tr>
<tr>
<td>RTT</td>
<td>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.</td>
</tr>
<tr>
<td>Encrypt Type</td>
<td>Encryption method performed on the data packets. The method is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• md5hash—MD5-based hashing encryption method</td>
</tr>
<tr>
<td></td>
<td>• none—No encryption</td>
</tr>
<tr>
<td></td>
<td>See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method performed by the GSS peer to prevent unauthorized access. The method is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• challenge—Challenge Handshake Authentication Protocol (CHAP)</td>
</tr>
<tr>
<td></td>
<td>• none—No secret string used for authentication</td>
</tr>
<tr>
<td></td>
<td>See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details.</td>
</tr>
<tr>
<td>KalFreq</td>
<td>Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user-configurable.</td>
</tr>
<tr>
<td>Max FrameSize</td>
<td>Maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user configurable.</td>
</tr>
<tr>
<td>OptmlFrameSize</td>
<td>Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.</td>
</tr>
<tr>
<td>PrePend</td>
<td>Allocated header size in the buffer. The header size is always 8 bytes.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>GSS ID</td>
<td>Unique identifier of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Connect from IP</td>
<td>Actual IP network address of the GSS peer in the mesh.</td>
</tr>
</tbody>
</table>
### Table 11-53 Field Descriptions for show sticky mesh verbose command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Local Address Via Peer</td>
<td>IP address of the local GSS node as seen by the GSS peer.</td>
</tr>
<tr>
<td>Last Up Event</td>
<td>Day and time of the most recent Up event.</td>
</tr>
<tr>
<td>Last Down Event</td>
<td>Day and time of the most recent Down event.</td>
</tr>
<tr>
<td>FSM Events</td>
<td>Finite State Machine events as related to the Session State field.</td>
</tr>
<tr>
<td>STOP</td>
<td>Number of SESSION_STOP events.</td>
</tr>
<tr>
<td>INIT</td>
<td>Number of SESSION_INIT events.</td>
</tr>
<tr>
<td>OPEN</td>
<td>Number of SESSION_OPEN events.</td>
</tr>
<tr>
<td>AUTH</td>
<td>Number of SESSION_AUTH events.</td>
</tr>
<tr>
<td>UP</td>
<td>Number of SESSION_UP events.</td>
</tr>
<tr>
<td>DOWN</td>
<td>Number of SESSION_DOWN events.</td>
</tr>
</tbody>
</table>

Table 11-54 describes the fields in the **show sticky mesh verbose** command output.

### Table 11-54 Field Descriptions for show sticky mesh verbose command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Information for...</td>
<td>Status and statistics about the global sticky mesh.</td>
</tr>
<tr>
<td>My GSS ID</td>
<td>Unique identifier of the local GSS node in the mesh.</td>
</tr>
<tr>
<td>Mesh ID</td>
<td>Unique identifier of the global sticky mesh.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user configurable.</td>
</tr>
</tbody>
</table>
| Encrypt Type                 | Encryption method performed on the data packets. The method is one of the following:  
|                              | • md5hash—MD5-based hashing encryption method                               |
|                              | • none—No encryption                                                       |
|                              | See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details. |
| Authentication                | Authentication method performed by GSS peers to prevent unauthorized access. The method is one of the following:  
|                              | • challenge—Challenge Handshake Authentication Protocol (CHAP)               |
|                              | • none—No secret string used for authentication                            |
|                              | See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details. |
| 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. |
### Table 11-54  Field Descriptions for show sticky mesh verbose Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OptimalFrameSize</td>
<td>Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.</td>
</tr>
<tr>
<td>Max Rate</td>
<td>Maximum rate that the local GSS node can transmit packets to GSS peers in the mesh.</td>
</tr>
<tr>
<td>Favored Peer</td>
<td>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.”</td>
</tr>
<tr>
<td>Session Information for</td>
<td>Status and statistics for a specific GSS peer in the mesh.</td>
</tr>
<tr>
<td>GSS peer</td>
<td></td>
</tr>
<tr>
<td>Session ID</td>
<td>Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.</td>
</tr>
<tr>
<td>Session State</td>
<td>State of the communication link between the local GSS node and the mesh peer. The possible states are as follows:</td>
</tr>
<tr>
<td></td>
<td>- SESSION_STOP—Indicates that the session is dead.</td>
</tr>
<tr>
<td></td>
<td>- SESSION_INIT—Indicates that the session is initializing.</td>
</tr>
<tr>
<td></td>
<td>- SESSION_OPEN—Indicates that the connection to the peer has been made.</td>
</tr>
<tr>
<td></td>
<td>- SESSION_AUTH—Indicates that authentication is occurring.</td>
</tr>
<tr>
<td></td>
<td>- SESSION_UP—Indicates that the session is up.</td>
</tr>
<tr>
<td></td>
<td>- SESSION_DOWN—Indicates that the session is down or failing.</td>
</tr>
<tr>
<td>RTT</td>
<td>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.</td>
</tr>
<tr>
<td>Encrypt Type</td>
<td>Encryption method performed on the data packets. The method is one of the following:</td>
</tr>
<tr>
<td></td>
<td>- md5hash—MD5-based hashing encryption method</td>
</tr>
<tr>
<td></td>
<td>- none—No encryption</td>
</tr>
<tr>
<td></td>
<td>See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method performed by GSS peers to prevent unauthorized access. The method is one of the following:</td>
</tr>
<tr>
<td></td>
<td>- challenge—Challenge Handshake Authentication Protocol (CHAP)</td>
</tr>
<tr>
<td></td>
<td>- none—No secret string used for authentication</td>
</tr>
<tr>
<td></td>
<td>See the “Configuring the Global Sticky Mesh” section in Chapter 9, Configuring DNS Sticky, for details.</td>
</tr>
<tr>
<td>KalFreq</td>
<td>Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user configurable.</td>
</tr>
<tr>
<td>Max FrameSize</td>
<td>Maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user configurable.</td>
</tr>
</tbody>
</table>
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

Monitoring GSS Global Server Load-Balancing Statistics from the CLI

Table 11-55  Field Descriptions for show sticky group-summary Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OptmFrameSize</td>
<td>Optimal frame size for communication between GSS devices in the mesh. This parameter is not user configurable.</td>
</tr>
<tr>
<td>PrePend</td>
<td>Allocated header size in the buffer. The header size is always 8 bytes.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>GSS ID</td>
<td>Unique identifier of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>Connect from IP</td>
<td>Actual IP network address of the GSS peer in the mesh.</td>
</tr>
<tr>
<td>My Local Address Via Peer</td>
<td>IP address of the local GSS node as seen by the GSS peer.</td>
</tr>
<tr>
<td>Last Up Event</td>
<td>Day and time of the most recent Up event.</td>
</tr>
<tr>
<td>Last Down Event</td>
<td>Day and time of the most recent Down event.</td>
</tr>
<tr>
<td>FSM Events</td>
<td>Finite State Machine events as related to the Session State field.</td>
</tr>
<tr>
<td>STOP</td>
<td>Number of SESSION_STOP events.</td>
</tr>
<tr>
<td>INIT</td>
<td>Number of SESSION_INIT events.</td>
</tr>
<tr>
<td>OPEN</td>
<td>Number of SESSION_OPEN events.</td>
</tr>
<tr>
<td>AUTH</td>
<td>Number of SESSION_AUTH events.</td>
</tr>
<tr>
<td>UP</td>
<td>Number of SESSION_UP events.</td>
</tr>
<tr>
<td>DOWN</td>
<td>Number of SESSION_DOWN events.</td>
</tr>
</tbody>
</table>

Displaying Sticky Group Configuration

You display a summary of all configured sticky groups by using the `show sticky group-summary` command.

Table 11-55 describes the fields in the `show sticky group-summary` command output.

Table 11-55  Field Descriptions for show sticky group-summary Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique alphanumeric name of the DNS sticky group.</td>
</tr>
<tr>
<td>Address Blocks</td>
<td>IP address block of the sticky group, specified in dotted-decimal notation.</td>
</tr>
</tbody>
</table>

You display the configuration of a specific sticky group by using the `show sticky group-name` command.

The syntax of this command is as follows:

```
show sticky group-name groupname
```

Enter the exact name of a sticky group to display all sticky entries related to that group.

Table 11-56 describes the fields in the `show sticky group-name` command output.
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 of the `clear statistics` command is as follows:

```
clear statistics {boomerang | ddos [all | attacks | drops | global] | dns | drpagent | keepalive [all | cra | http-head | https-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.
- **https-head**—Resets statistics for only the VIP HTTPS-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
```

**Monitoring Global Load-Balancing Statistics from the Primary GSSM GUI**

From the Monitoring tab of the primary GSSM GUI, you can monitor 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 monitor advanced traffic management functions, such as DNS sticky and network proximity, for the GSS network.

This section contains the following topics:

- Monitoring Answer Status and Statistics
- Monitoring DNS Rule Statistics
- Monitoring Domain Hit Counts
- Monitoring Global Statistics
- Monitoring Source Address Statistics
- Monitoring DDoS Statistics
- Monitoring Traffic Management Statistics

**Monitoring 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:

- Monitoring Answer Hit Counts
- Monitoring Answer Keepalive Statistics
- Monitoring Answer Status

**Monitoring 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 view 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. The Answer Status list page appears displaying the following information:

   Data displayed in the Answer Status list page may be delayed by up to 300 seconds.

3. Click the Answer Hit Counts navigation link (located in the Contents list). The Answer Hit Counts list page appears.

Table 11-57 describes the fields on the Answer Hit Counts list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer IP address</td>
<td>IP address of the answer resource. You get either an IPv4 or an IPv6 address for the VIP-type answers, and you get only IPv4 address for the NS and CRA-type answers.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the answer using the primary GSSM GUI.</td>
</tr>
<tr>
<td>Type</td>
<td>Resources to which the GSS resolves DNS requests. The answer types include VIP, CRA, or Name Server.</td>
</tr>
<tr>
<td>Location</td>
<td>GSS network location of the answer.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>Number of requests directed to the answer by each GSS device.</td>
</tr>
</tbody>
</table>

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

**Monitoring 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. When you use a TCP keepalive with the fast detection and graceful termination methods to test a Telnet service on a server running Windows Server 2003, port 23 may fluctuate between the Up and Down state (port flapping). If port flapping occurs on TCP port 23 of Windows Server 2003, you will notice an increase in keepalive negative probe and keepalive transition counts on the Answer Keepalive Statistics list page of the primary GSSM GUI.

To resolve this issue, increase the retries value for the TCP keepalive. A retry value of 3 or 4 should prevent flapping on port 23 when connecting to a server running Windows Server 2003.

To view 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.

3. Click the Answer KeepAlive Statistics navigation link (located in the Contents list). The Answer KeepAlive Statistics list page appears.
Table 11-58  describes the fields on the Answer KeepAlive Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer</td>
<td>IP address of the answer resource probed by the GSS.</td>
</tr>
<tr>
<td>Type</td>
<td>Resources to which the GSS resolves DNS requests. Answer types include VIP,</td>
</tr>
<tr>
<td></td>
<td>CRA, or Name Server.</td>
</tr>
<tr>
<td>Name</td>
<td>Name assigned to the answer using the primary GSSM GUI.</td>
</tr>
<tr>
<td>Keepalive</td>
<td>Address assigned to the remote device, CRA, or name server that the GSS</td>
</tr>
<tr>
<td></td>
<td>is to forward requests.</td>
</tr>
<tr>
<td>Method</td>
<td>Keepalive method used by the answer: VIP (virtual IP address), NS (name</td>
</tr>
<tr>
<td></td>
<td>server), or CRA (content routing agent).</td>
</tr>
<tr>
<td>Location</td>
<td>GSS network location of the answer.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>Number of keepalive probes directed to the answer by each GSS device and</td>
</tr>
<tr>
<td></td>
<td>the record of how those probes were handled. Statistics are presented in</td>
</tr>
<tr>
<td></td>
<td>the following order:</td>
</tr>
<tr>
<td></td>
<td>• Keepalive packets sent—Total number of keepalive probes sent to the</td>
</tr>
<tr>
<td></td>
<td>answer by each GSS on the network</td>
</tr>
<tr>
<td></td>
<td>• Keepalive packets received—Total number of keepalive probes returned</td>
</tr>
<tr>
<td></td>
<td>from the answer</td>
</tr>
<tr>
<td></td>
<td>• Keepalive positive probe count—Total number of keepalive probes</td>
</tr>
<tr>
<td></td>
<td>received by the GSS to which a positive (OK) response was returned</td>
</tr>
<tr>
<td></td>
<td>• Keepalive negative probe count—Total number of keepalive probes</td>
</tr>
<tr>
<td></td>
<td>received by the GSS to which a negative response was returned</td>
</tr>
<tr>
<td></td>
<td>• Keepalive transition count—Total number of keepalive probe transitions</td>
</tr>
<tr>
<td></td>
<td>(for example, from the INIT to the ONLINE state) experienced by the</td>
</tr>
<tr>
<td></td>
<td>keepalive</td>
</tr>
</tbody>
</table>

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

**Monitoring 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 view 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.

Table 11-59 describes the fields on the Answer Status list page.
Chapter 11      Monitoring GSS Global Server Load-Balancing Operation

Monitoring 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 view 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.

Table 11-60 describes the fields on the DNS Rule Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name assigned to the answer using the primary GSSM.</td>
</tr>
<tr>
<td>Owner</td>
<td>GSS owner to whom the DNS rule has been assigned.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>Total hit count and successful hit count for the DNS rule from the listed GSS device. See 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.</td>
</tr>
</tbody>
</table>

3. Click the column header of any of the displayed columns to sort your DNS rules by a particular property.

Monitoring 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 view the status of your hosted domains, perform the following steps:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Domains** navigation link. The Domain Hit Counts list page appears.

Table 11-61 describes the fields on the Domain Hit Counts list page.

### Table 11-61  Field Descriptions for Domain Hit Counts List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>DNS domains for which the GSS is responsible. These are the domains contained in your domain lists.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>Total number of requests for the listed domain from each GSS device.</td>
</tr>
</tbody>
</table>

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

### Monitoring 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 and the online status of each GSS device.

To view 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 appears.

Table 11-62 describes the fields on the Global Statistics list page.

### Table 11-62  Field Descriptions for Global Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSS Status</td>
<td>Online status of each GSS device in your GSS network.</td>
</tr>
<tr>
<td>Unmatched DNS Queries</td>
<td>Total number of DNS queries received by each listed device for which no answer could be found.</td>
</tr>
<tr>
<td>DNS Queries/sec</td>
<td>Average number of DNS queries received, per second, by each listed GSS device.</td>
</tr>
<tr>
<td>Keepalive Probes/sec</td>
<td>Average number of keepalive probes received by each listed GSS device each second.</td>
</tr>
</tbody>
</table>

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.
Monitoring 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 view 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. Table 11-63 describes the fields on the Source Address Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address Block</td>
<td>Address or range of addresses that originate the DNS queries. Source address blocks make up GSS source address lists.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>Total number of requests received by the listed GSS device from each source address or address block.</td>
</tr>
</tbody>
</table>

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

Monitoring 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 view 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 submenu items, Global Stats and Attack Stats.
3. Click the Global Stats selection to view the DDoS Global Statistics. Table 11-64 describes the fields on the Global Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total packets received</td>
<td>Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.</td>
</tr>
<tr>
<td>Total packets dropped</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.</td>
</tr>
<tr>
<td>Total Anti-Spoofing triggered</td>
<td>The total number of packets that triggered the GSS DDoS protection anti-spoofing function.</td>
</tr>
<tr>
<td>Total Validated DNS requests</td>
<td>Total number of packets that were successfully dropped by the GSS DDoS protection anti-spoofing function.</td>
</tr>
</tbody>
</table>
### Table 11-64  Field Descriptions for Global Statistics List Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate-limit drops</td>
<td>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.</td>
</tr>
<tr>
<td>Global Rate-limit drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.</td>
</tr>
<tr>
<td>Unknown dproxies drops</td>
<td>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.</td>
</tr>
<tr>
<td>Spoofed packet drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an attack and dropped.</td>
</tr>
<tr>
<td>Malformed packet drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as malformed and dropped.</td>
</tr>
<tr>
<td>Mitigation rules drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.</td>
</tr>
<tr>
<td>Global domain name drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.</td>
</tr>
<tr>
<td>Ongoing anti-spoofing drops</td>
<td>Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.</td>
</tr>
<tr>
<td>DDoS Status</td>
<td>DDoS detection and mitigation module status on the GSS, either enabled or disabled.</td>
</tr>
</tbody>
</table>

4. Click the **Attack Stats** selection to view the DDoS Attack Statistics.

### Table 11-65  Field Descriptions for Attack Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total attacks</td>
<td>Total number of DNS attacks detected by the GSS.</td>
</tr>
<tr>
<td>Reflection attacks</td>
<td>Attack in which the IP address of the victim (i.e., the GSS) is spoofed and multiple DNS requests are sent to a DNS server or multiple DNS servers posing as the victim.</td>
</tr>
<tr>
<td>Malformed DNS packet attacks</td>
<td>Attack in which the GSS is flooded with malformed DNS packets.</td>
</tr>
<tr>
<td>Failed global domain attacks</td>
<td>Failed domain counter that provides a total of the DNS queries failing to match the global domain name.</td>
</tr>
<tr>
<td>Global rate-limit exceeded attacks</td>
<td>Attack in which the maximum number of DNS requests that the GSS receives from the D-proxy per second exceeds the global limit.</td>
</tr>
<tr>
<td>DDoS status</td>
<td>DDoS detection and mitigation module status on the GSS, either enabled or disabled.</td>
</tr>
</tbody>
</table>
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:

- Monitoring Proximity Rule Hit Count Statistics
- Monitoring Proximity Database Statistics
- Monitoring Proximity Lookup Statistics
- Monitoring Proximity Probe Management Statistics
- Monitoring Sticky Rule Hit Statistics
- Monitoring Sticky Database Statistics
- Monitoring Global Sticky Mesh Statistics

Monitoring 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 view 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.

Table 11-66 describes the fields on the Proximity Rule Hit Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the matched DNS rule.</td>
</tr>
<tr>
<td>Owner</td>
<td>GSS owner to whom the DNS rule has been assigned.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>For each GSS or GSSM, this field provides information about the number of:</td>
</tr>
<tr>
<td></td>
<td>• DNS requests that match the DNS rule.</td>
</tr>
<tr>
<td></td>
<td>• DNS responses that are successfully returned with a proximate answer for the DNS rule.</td>
</tr>
<tr>
<td></td>
<td>See 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.</td>
</tr>
</tbody>
</table>
Monitoring 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 view 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.

Table 11-67 describes the fields on the Proximity Database Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Site Selector</td>
<td>Name of the GSS or GSSM device.</td>
</tr>
<tr>
<td>Entries in Use</td>
<td>Number of entries currently in the proximity database, out of a maximum of 500,000 entries.</td>
</tr>
<tr>
<td>Last Cleanup</td>
<td>Last time the GSS removed the least recently used entries from the proximity database.</td>
</tr>
<tr>
<td>Number of Cleanups</td>
<td>Number of entries removed during the cleanup process.</td>
</tr>
</tbody>
</table>

Monitoring Proximity Lookup Statistics

The Proximity Lookup Statistics list page displays statistics about the number of entries in the proximity database:

To view 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.

Table 11-68 describes the fields on the Proximity Lookup Statistics list page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Site Selector</td>
<td>Name of the GSS or GSSM device</td>
</tr>
<tr>
<td>Count</td>
<td>Total number of proximity lookup requests made to the GSS.</td>
</tr>
<tr>
<td>Crnt Rate</td>
<td>Current request rate per second that requests are made to the GSS to perform a proximity lookup in the database.</td>
</tr>
<tr>
<td>No Entry</td>
<td>Number of times the GSS was unable to locate a proximate answer from the proximity database.</td>
</tr>
<tr>
<td>Partial Data</td>
<td>Number of times only round-trip time (RTT) data for a partial set of zones was available in the proximity database.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring GSS Global Server Load-Balancing Operation

Monitoring Global Load-Balancing Statistics from the Primary GSSM GUI

Table 11-68  Field Descriptions for Proximity Lookup Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req. Dropped</td>
<td>Number of proximity lookup queries dropped by the GSS.</td>
</tr>
<tr>
<td>Db Full</td>
<td>Number of times the GSS was unable to perform a proximity add because the database exceeded the maximum number of entries.</td>
</tr>
</tbody>
</table>

Monitoring Proximity Probe Management Statistics

The Proximity Probe Management Statistics list page displays statistics about the ICMP and TCP probes transmitted from the proximity probing agents.

To view 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.

Table 11-69 describes the fields on the Proximity Probe Mgmt Statistics list page.

Table 11-69  Field Descriptions for Proximity Probe Mgmt Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Index</td>
<td>Numerical identifier of the proximity zone.</td>
</tr>
<tr>
<td>Zone Name</td>
<td>Name of the proximity zone.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>For each GSS or GSSM, this field provides information on the:</td>
</tr>
<tr>
<td></td>
<td>• IP address of the probe device.</td>
</tr>
<tr>
<td></td>
<td>• Total number of DRP echo and measurement packets sent by the GSS to the proximity probing agent in the proximity zone.</td>
</tr>
<tr>
<td></td>
<td>• Total number of DRP echo and measurement packets received by the GSS from the proximity probing agent in the proximity zone.</td>
</tr>
<tr>
<td></td>
<td>• Current packet send rate per second.</td>
</tr>
</tbody>
</table>

See 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.

Monitoring Sticky Rule Hit Statistics

The Sticky Rule Hit Statistics list page displays statistics about 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 view 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.
Table 11-70 describes the fields on the Sticky Rule Hit Statistics list page.

### Field Descriptions for Sticky Rule Hit Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the matched DNS rule.</td>
</tr>
<tr>
<td>Owner</td>
<td>GSS owner to whom the DNS rule has been assigned.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM</td>
<td>For each GSS or GSSM:</td>
</tr>
<tr>
<td></td>
<td>- The total number of successful sticky answer matches in the sticky</td>
</tr>
<tr>
<td></td>
<td>database for the DNS rule.</td>
</tr>
<tr>
<td></td>
<td>- The total number of failed sticky answer lookups in the sticky</td>
</tr>
<tr>
<td></td>
<td>database for the DNS rule.</td>
</tr>
<tr>
<td></td>
<td>See the legend that appears below the listed DNS rules for information</td>
</tr>
<tr>
<td></td>
<td>about identifying which value represents successful matches and which</td>
</tr>
<tr>
<td></td>
<td>value represents failed lookups.</td>
</tr>
</tbody>
</table>

### Monitoring Sticky Database Statistics

The Sticky Database Statistics list page displays statistics about the number of entries in the sticky database.

To view 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.

Table 11-71 describes the fields on the Sticky Database Statistics list page.

### Field Descriptions for Sticky Database Statistics List Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Site Selector</td>
<td>Name of the GSS device (GSSM or GSS).</td>
</tr>
<tr>
<td>Status</td>
<td>Sticky status of the named device and sticky mode. Status conditions can</td>
</tr>
<tr>
<td></td>
<td>include Disabled, Local, Global, and Stopped.</td>
</tr>
<tr>
<td>Entries in Use</td>
<td>Number of entries currently in the sticky database out of a maximum of</td>
</tr>
<tr>
<td></td>
<td>400,000 entries.</td>
</tr>
</tbody>
</table>

### Monitoring 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.

Table 11-72 describes the fields on the Sticky Mesh Statistics list page.

**Table 11-72 Field Descriptions for Sticky Mesh Statistics List Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSS/Peer</td>
<td>Name of the GSS device (GSSM or GSS) in the mesh along with its peers.</td>
</tr>
<tr>
<td>Name of the GSS or GSSM in the mesh</td>
<td>For each GSS peer in the mesh, each column lists the following statistics:</td>
</tr>
<tr>
<td></td>
<td>• Connection to peer status—Online status of each peer in the mesh. The possible states are Stopped, Init, Opened, Authentication, Up, and Down.</td>
</tr>
<tr>
<td></td>
<td>• Packets transmitted—Number of packets transmitted from the GSS or GSSM to each peer in the mesh.</td>
</tr>
<tr>
<td></td>
<td>• Packets received—Number of packets received by the GSS or GSSM from each peer in the mesh.</td>
</tr>
<tr>
<td></td>
<td>• Down Events—The number of down events encountered for the session between the peers in the mesh.</td>
</tr>
<tr>
<td></td>
<td>See 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.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid answer name. If entered, name must not be the empty string.</td>
<td>You entered an invalid name for the answer. Answer names cannot be blank or contain blank spaces.</td>
<td>Enter a valid alphanumeric answer name between 1 and 80 characters that does not contain spaces.</td>
</tr>
<tr>
<td>Invalid answer name. Name length must not exceed 80 characters.</td>
<td>You entered an answer name that contains too many characters.</td>
<td>Enter a valid alphanumeric answer name between 1 and 80 characters that does not contain spaces.</td>
</tr>
<tr>
<td>Invalid CRA timing decay. Timing decay must be between 1 and 10.</td>
<td>You entered an invalid number for the CRA timing decay.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid CRA static RTT value. Static RTT must be between 0 and 1000.</td>
<td>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.</td>
<td>Enter a static RTT value between 0 and 1000.</td>
</tr>
<tr>
<td>A VIP/Name Server/CRA-type answer named answer_name already exists. If specified, name and type must uniquely identify an answer.</td>
<td>You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and answer type.</td>
<td>Assign a new name or answer type to your answer to make it unique.</td>
</tr>
<tr>
<td>An unnamed VIP/Name Server/CRA-type answer having address IP_address already exists. Name must be specified to configure an answer with the same address as another answer.</td>
<td>You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and IP address.</td>
<td>Assign a new name to your answer to make it unique.</td>
</tr>
<tr>
<td>The maximum number of number VIP/Name Server/CRA-type answers has been met.</td>
<td>You attempted to create an answer when the maximum number of that type of answer has already been created.</td>
<td>Remove an existing answer of the same type.</td>
</tr>
<tr>
<td>CRA decay value must be specified.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table A-1  Answer Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRA static RTT must be specified.</td>
<td>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.</td>
<td>Enter a number between 1 and 1000 for the CRA round-trip time in milliseconds.</td>
</tr>
<tr>
<td>Invalid keepalive tag. Tag must be at least one character in length.</td>
<td>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.</td>
<td>Enter an alphanumeric tag between 1 and 76 characters in the Tag field.</td>
</tr>
<tr>
<td>Invalid keepalive tag. Tag length must not exceed 76 characters.</td>
<td>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.</td>
<td>Enter an alphanumeric tag between 1 and 76 characters in the Tag field.</td>
</tr>
<tr>
<td>NS-type answer IP Address has the same IP address as GSS GSS_name. GSS IP addresses must not equal any NS-type answers.</td>
<td>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.</td>
<td>Assign a valid IP address to your name server answer.</td>
</tr>
<tr>
<td>Invalid answer order. Order must not be negative.</td>
<td>You attempted to assign a negative order number to your answer. The order must be a positive number.</td>
<td>Enter a nonnegative whole number for the order.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>This answer group cannot be deleted because it is referenced by number DNS rule balance clause(s).</td>
<td>You attempted to delete an answer group that is being referenced by one or more DNS rules.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid answer group name. Name must be entered.</td>
<td>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.</td>
<td>Enter a name for the new answer group in the field provided, and then click Save.</td>
</tr>
</tbody>
</table>
### Table A-2 Answer Group Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid answer group name. Name length must not exceed 80 characters.</td>
<td>You attempted to assign an invalid name to the answer group.</td>
<td>Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.</td>
</tr>
<tr>
<td>Invalid answer group name. Name must not contain spaces.</td>
<td>You attempted to assign an invalid name to the answer group.</td>
<td>Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.</td>
</tr>
<tr>
<td>An answer group named <code>name</code> already exists. Name must uniquely identify an answer group.</td>
<td>You attempted to assign the answer group a name that is already being used by a different GSS device.</td>
<td>Enter a unique alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.</td>
</tr>
<tr>
<td>The maximum number of number answers per VIP/Name Server/CRA-type group has been met.</td>
<td>You attempted to add an answer to an answer group to which the maximum number of answers has already been assigned.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid answer load threshold. Load threshold must be between 2 and 254.</td>
<td>You attempted to assign an invalid load threshold to your answer in the LT field.</td>
<td>Assign a load threshold for the answer that is between 2 and 254 in the LT field.</td>
</tr>
</tbody>
</table>
## Domain List Error Messages

Table A-3 lists the potential error messages that may appear when configuring domain lists.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;domain name&gt;</code> must contain at least one character.</td>
<td>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.</td>
<td>Enter a name that is between 1 and 100 characters and then save your domain list.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> character limit exceeded.</td>
<td>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.</td>
<td>Enter a new domain name of no more than 100 characters and then save your domain list.</td>
</tr>
<tr>
<td>Domain specification must not exceed 128 characters.</td>
<td>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.</td>
<td>Replace the domain with a domain name containing fewer than 128 characters and then save your domain list.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> must not contain spaces.</td>
<td>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.</td>
<td>Modify the domain name so that it does not contain spaces and then save your domain list.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> is not a valid regular expression: <code>&lt;regular expression syntax error message here&gt;</code></td>
<td>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.</td>
<td>Modify the domain name so that it is a valid regular expression and does not contain any invalid characters or formatting (for example, <a href="http://www.cisco.com">www.cisco.com</a> or *.cisco*.com), and then save your domain list.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> must not begin or end with `.'</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> component must not begin or end with <code>'-</code></td>
<td>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, <a href="http://www.cisco-.com">www.cisco-.com</a>).</td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;domain name&gt;</code> contains invalid character <code>'&lt;character&gt;'</code> (&lt;ASCII value of the character&gt;)</td>
<td>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.</td>
<td>Modify the domain name so that it does not contain an invalid text character and then save your domain list.</td>
</tr>
</tbody>
</table>
## Domain List Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>This domain list cannot be deleted because it is referenced by X DNS rule</td>
<td>You attempted to delete a domain list that is being referenced by one or more DNS rules.</td>
<td>Modify any DNS rules that use the domain list so that they no longer reference it and then try again to delete the list.</td>
</tr>
<tr>
<td>Invalid domain list name. Name must be entered.</td>
<td>You attempted to create a domain list without a name. Domain lists must have names of at least one character.</td>
<td>Assign a name that has between 1 and 80 characters to your domain list and then save it.</td>
</tr>
<tr>
<td>Invalid domain list name. Name length must not exceed 80 characters.</td>
<td>You attempted to create a domain list with a name that is too long.</td>
<td>Assign a name that has between 1 and 80 characters to your domain list and then save it.</td>
</tr>
<tr>
<td>Invalid domain list name. Name must not contain spaces.</td>
<td>You attempted to create a domain list with a name that contains spaces. Domain list names cannot contain spaces.</td>
<td>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.</td>
</tr>
<tr>
<td>A domain list named '&lt;name&gt;' already exists. Name must uniquely identify a domain list.</td>
<td>You attempted to assign a name to your domain list that has already been assigned to another domain list on the same GSS network.</td>
<td>Assign a unique name to your new domain list and then save the list.</td>
</tr>
<tr>
<td>The maximum number of &lt;limit&gt; domains per list has been met.</td>
<td>You attempted to add a domain to your domain list when the maximum number of domains has already been added to that list.</td>
<td>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.</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL must be specified for balance method associated with CRA- or VIP-type answer group.</td>
<td>You attempted to create a balance clause without specifying a Time To Live (TTL) for answers returned by the clause.</td>
<td>Enter a TTL value between 0 and 604,800 seconds.</td>
</tr>
<tr>
<td>Invalid balance clause TTL. TTL must be between 0 and 604,800.</td>
<td>You attempted to create a balance clause with an incorrect TTL value for answers provided by the balance clause.</td>
<td>Enter a TTL value between 0 and 604,800 seconds.</td>
</tr>
<tr>
<td>Invalid balance clause position. Position must be between 0 and 2.</td>
<td>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.</td>
<td>Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order with no gaps between them.</td>
</tr>
<tr>
<td>Hash type must be specified for answer group using hash balance method.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Balance clause boomerang fragment size must be specified.</td>
<td>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.</td>
<td>Enter a fragment size between 28 and 1980 in the field provided. The fragment size must be divisible by 4.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang fragment size. Boomerang fragment size must be 0 or between 28 and 1980.</td>
<td>You attempted to specify an unacceptable fragment size for this balance clause in the Fragment Size field.</td>
<td>Enter a valid fragment size. Fragment sizes must be between 28 and 1980 and must be divisible by 4.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang fragment size. Boomerang fragment size must be a multiple of 4.</td>
<td>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.</td>
<td>Enter a fragment size between 28 and 1980 that is also divisible by 4. Zero is also an acceptable fragment size.</td>
</tr>
</tbody>
</table>
### DNS Rule Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance clause Boomerang IP TTL value must be specified.</td>
<td>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.</td>
<td>Enter an IP TTL between 1 and 255 in the field provided and then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang IP TTL. Boomerang IP TTL must be between 1 and 255.</td>
<td>You attempted to create a balance clause using the boomerang balance method but have specified an invalid IP Time to Live (TTL).</td>
<td>Enter an IP TTL between 1 and 255 in the field provided and then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Balance clause Boomerang maximum propagation delay must be specified.</td>
<td>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).</td>
<td>Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang maximum propagation delay. Boomerang maximum propagation delay must be between 1 and 1000.</td>
<td>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.</td>
<td>Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.</td>
</tr>
<tr>
<td>Balance clause Boomerang padding size must be specified.</td>
<td>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.</td>
<td>Enter a valid pad size between 0 and 2000 in the Pad Size field.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang padding size. Boomerang padding size must be between 0 and 2000.</td>
<td>You attempted to create a balance clause using the boomerang balance method but have specified an invalid pad size in the Pad Size field.</td>
<td>Enter a valid pad size between 0 and 2000 in the Pad Size field.</td>
</tr>
</tbody>
</table>
### Table A-4 DNS Rule Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid balance clause Boomerang secret. If specified, Boomerang secret must be between 1 and 64 characters in length.</td>
<td>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.</td>
<td>Enter a valid boomerang secret between 1 and 64 characters in the Secret field.</td>
</tr>
<tr>
<td>Balance clause Boomerang server delay must be specified.</td>
<td>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.</td>
<td>Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.</td>
</tr>
<tr>
<td>Invalid balance clause Boomerang server delay. Boomerang server delay must be between 32 and 999.</td>
<td>You attempted to create a balance clause using the boomerang balance method but have specified an invalid server delay in the Server Delay field.</td>
<td>Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.</td>
</tr>
<tr>
<td>Invalid DNS rule name. Name must be entered.</td>
<td>You attempted to create a DNS rule without assigning a name to the rule. DNS rules must have names between 1 and 100 characters.</td>
<td>Assign a name to your DNS rule using the Rule Name field and then try again to save the rule.</td>
</tr>
<tr>
<td>Invalid DNS rule name. Name length must not exceed 100 characters.</td>
<td>You attempted to assign a name to your DNS rule that is too long. The maximum length for DNS rules is 100 characters.</td>
<td>Enter a name for your DNS rule that is between 1 and 100 characters and then attempt to save the rule again.</td>
</tr>
<tr>
<td>Invalid DNS rule name. Name must not contain spaces.</td>
<td>You attempted to assign your DNS rule a name that contains spaces.</td>
<td>Enter a valid name for your DNS rule that is between 1 and 100 characters and does not contain spaces.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
<td>Reconfigure your DNS rule so that it does not exactly match the preexisting rule and then save the rule.</td>
</tr>
</tbody>
</table>
### DNS Rule Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate answer group/balance method assignment detected. A DNS rule cannot use the same answer group and balance method in multiple balance clauses.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Balance clause gap detected at position (0,1,2). Balance clauses must be specified sequentially without gaps.</td>
<td>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.</td>
<td>Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order with no gaps between them.</td>
</tr>
<tr>
<td>A DNS rule named DNS_Rule_name already exists. Name must uniquely identify a DNS rule.</td>
<td>You attempted to assign a name to the DNS rule that is already assigned to another rule. DNS rule names must be unique.</td>
<td>Assign a rule to the name that is not already being used and then save the rule.</td>
</tr>
<tr>
<td>Balance clause 1/2 cannot be sticky because clause number 0/1 is not sticky.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid balance method. Proximity cannot be enabled for balance method Hashed.</td>
<td>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.</td>
<td>Choose a different balance method for the answer group from the Select Balance Method drop-down list.</td>
</tr>
</tbody>
</table>
# KeepAlive Error Messages

Table A-5 lists the potential error messages that may appear when configuring keepalives.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid CAPP hash secret. Secret must be entered.</td>
<td>You attempted to create a KAL-AP keepalive using a CAPP hash secret but have not specified a secret in the field provided.</td>
<td>Enter a CAPP hash secret of no more than 31 characters in the field provided.</td>
</tr>
<tr>
<td>Invalid CAPP hash secret. Secret length must not exceed 31 characters.</td>
<td>You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.</td>
<td>Enter a CAPP hash secret of no more than 31 characters in the field provided.</td>
</tr>
<tr>
<td>Invalid HTTP HEAD response timeout.</td>
<td>You attempted to specify an HTTP HEAD response timeout that is invalid.</td>
<td>Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.</td>
</tr>
<tr>
<td>Response timeout must be between 20 and 60 seconds.</td>
<td>You attempted to specify an HTTP HEAD response timeout that is invalid.</td>
<td>Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.</td>
</tr>
<tr>
<td>Invalid HTTP HEAD destination port. Destination port must be between 1 and 65,535.</td>
<td>You attempted to specify a port number for HTTP HEAD traffic that is invalid.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid HTTP HEAD path. Path length must not exceed 256 characters.</td>
<td>You attempted to specify an HTTP HEAD path that is not valid.</td>
<td>Enter a valid path shorter than 256 characters in the HTTP HEAD default path field in the Shared Keepalive details page.</td>
</tr>
<tr>
<td>Invalid &lt;keepalive type&gt; minimum probe frequency. Frequency must be between &lt;min&gt; and &lt;max&gt;.</td>
<td>You attempted to specify a minimum probe interval for your keepalive type that is invalid.</td>
<td>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.</td>
</tr>
<tr>
<td>Duplicate keepalive address detected. A keepalive must not be configured to use the same primary and secondary addresses.</td>
<td>You attempted to configure a KAL-AP keepalive that is identical to a keepalive of the same type that already exists.</td>
<td>Configure the KAL-AP keepalive to use a different primary and secondary address.</td>
</tr>
<tr>
<td>Duplicate keepalive primary address 'primaryaddress' detected. An address can be used by at most one KAL-AP type keepalive.</td>
<td>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.</td>
<td>Configure the KAL-AP keepalive to use a primary IP address that is not already being used by another keepalive.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Description</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Duplicate keepalive secondary address '&lt;secondary address&gt;' detected. An address can be used by at most one KAL-AP type keepalive.</td>
<td>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.</td>
<td>Configure the KAL-AP keepalive to use a secondary IP address that is not already being used by another keepalive.</td>
</tr>
<tr>
<td>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.</td>
<td>You attempted to configure an HTTP HEAD keepalive that features an identical configuration to that of another HTTP HEAD keepalive on your GSS network.</td>
<td>Configure the HTTP HEAD keepalive to use a unique configuration of address, destination path, host tag, and port.</td>
</tr>
<tr>
<td>Duplicate keepalive detected. An ICMP keepalive must not use the same address as another ICMP keepalive.</td>
<td>You attempted to configure an ICMP keepalive with an IP address that is identical to that of another ICMP keepalive on your GSS network.</td>
<td>Configure the ICMP to use a unique IP address.</td>
</tr>
<tr>
<td>Invalid CAPP hash secret. Secret length must not exceed 31 characters.</td>
<td>You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.</td>
<td>Enter a CAPP hash secret of no more than 31 characters in the field provided.</td>
</tr>
<tr>
<td>Invalid HTTP HEAD destination port. If specified, destination port must be between 0 and 65,535.</td>
<td>You attempted to specify a port number for HTTP HEAD traffic that is invalid.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid HTTP HEAD host tag. Host tag length must not exceed 128 characters.</td>
<td>You attempted to create an HTTP HEAD host tag that is too long.</td>
<td>Enter an HTTP HEAD host tag of no more than 128 characters.</td>
</tr>
</tbody>
</table>
Location Error Messages

Table A-6 lists the potential error messages that may appear when configuring locations.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The location is still being referenced by other objects and cannot be removed.</td>
<td>You attempted to delete a location that has answers or GSS devices associated with it.</td>
<td>Dissociate any answers or GSS devices from the location and then try again to delete it.</td>
</tr>
<tr>
<td>There already exists a location named &lt;name&gt; in region &lt;region&gt; with the same name. Please specify a different location name.</td>
<td>You attempted to create a location within this region when another location with the same name already exists.</td>
<td>Change the name of the location so that it is unique for the region.</td>
</tr>
</tbody>
</table>

Network Error Messages

Table A-7 lists the potential error messages that may appear when configuring the primary GSSM network.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of GSSMs exceeded. A GSS network can contain at most 2 GSSMs.</td>
<td>You attempted to enable a GSSM when there are already two GSSMs enabled on your GSS network.</td>
<td>If necessary, remove your standby GSSM from your GSS network and then try again to enable the GSSM.</td>
</tr>
<tr>
<td>The maximum number of &lt;size&gt; &lt;className&gt; has been met.</td>
<td>You attempted to add a resource to your GSS network when the maximum number of that resource already exists.</td>
<td>Remove an existing resource of the same type and then try again to add the new resource.</td>
</tr>
</tbody>
</table>

Owner Error Messages

Table A-8 lists the potential error messages that may appear when configuring owners.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid owner name. Name must be entered.</td>
<td>You attempted to create an owner without assigning a name to the owner.</td>
<td>Owners must have a unique name. Enter a name for the owner in the field provided and then save the owner.</td>
</tr>
<tr>
<td>Invalid owner name. Name length must not exceed 80 characters.</td>
<td>You attempted to assign a name to an owner that is too long.</td>
<td>Assign a name to your owner that is no longer than 80 characters.</td>
</tr>
<tr>
<td>An owner named &lt;owner name&gt; already exists. Name must uniquely identify an owner.</td>
<td>You attempted to assign a name to your owner that is already assigned to another owner on your GSS network.</td>
<td>Assign a unique name to your owner.</td>
</tr>
</tbody>
</table>
# Proximity Error Messages

Table A-9 lists the potential error messages that may appear when configuring network proximity.

## Table A-9 Proximity Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.</td>
<td>You entered an incorrect global subnet mask in the Global Proximity Configuration details page (Traffic Mgmt tab).</td>
<td>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).</td>
</tr>
<tr>
<td>Invalid Equivalence window. Equivalence window must be between 0 and 100</td>
<td>You entered an incorrect Equivalence Window value in the Global Proximity Configuration details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid Entry inactivity timeout. Entry inactivity timeout must be between 15 and 10080</td>
<td>You entered an incorrect Entry Inactivity Timeout value in the Global Proximity Configuration details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid Refresh probe interval. Refresh probe interval must be between 1 and 72</td>
<td>You entered an incorrect Refresh Probe Interval value in the Global Proximity Configuration details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid Acceptable RTT. Acceptable RTT must be between 50 and 500</td>
<td>You entered an incorrect acceptable RTT value in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table A-9 Proximity Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Acceptable percentage of available zones. Acceptable percentage of available zones must be between 3 and 100</td>
<td>You entered an incorrect proximity acceptable zone percentage in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid DRP key. Key must have an Id.</td>
<td>You attempted to create a DRP key without an ID value in the Creating New DRP Key details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid DRP key. Key must have a string.</td>
<td>You attempted to create a DRP key without a string in the Creating New DRP Key details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid key ID. Key with the ID 'xxx' already exists.</td>
<td>You attempted to create a DRP key that is using an existing DRP key ID.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid DRP Key Id. DRP Key Id must be between 0 and 255.</td>
<td>You entered an incorrect DRP key ID in the Creating New DRP Key details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid DRP Key String Length. DRP Key String Length must be between 1 and 80.</td>
<td>You entered an incorrect DRP key string in the Creating New DRP Key details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table A-9  Proximity Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid key String. Key String cannot start with a digit.</td>
<td>You attempted to create a DRP key that begins with a number.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid key String. Key String is limited to alphanumeric characters.</td>
<td>You attempted to create a DRP key with non-supported characters.</td>
<td>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.</td>
</tr>
<tr>
<td>The maximum of 32 DRP Key has been met.</td>
<td>The primary GSSM GUI supports a maximum of 32 keys.</td>
<td>If necessary, delete one or more DRP authentication keys from the primary GSSM GUI (see Chapter 10, Configuring Network Proximity).</td>
</tr>
<tr>
<td>Invalid Zone Index. Zone Index must be between 1 and 32.</td>
<td>You entered an incorrect proximity zone index in the Creating New Zone details page (Traffic Mgmt tab).</td>
<td>Enter an integer from 1 to 32 for the proximity zone Index. There is no default.</td>
</tr>
<tr>
<td>Invalid zone name. Zone with index 'xxx' already has the name 'yyy'.</td>
<td>You attempted to create a proximity zone that is using an existing zone name.</td>
<td>Enter a different description of the proximity zone. Only alphanumeric characters and the underscore (_) character are allowed.</td>
</tr>
<tr>
<td>Invalid zone index. Zone with the name 'yyy' already has index 'xxx'.</td>
<td>You attempted to create a proximity zone that is using an existing index.</td>
<td>Enter a different proximity zone index. Enter an integer from 1 to 32. There is no default.</td>
</tr>
<tr>
<td>The maximum of 32 Zones has been met.</td>
<td>The primary GSSM GUI supports a maximum of 32 proximity zones.</td>
<td>If necessary, delete one or more proximity zones from the primary GSSM GUI (see Chapter 10, Configuring Network Proximity).</td>
</tr>
<tr>
<td>Invalid probe device address. A probe device with address '1.2.3.4' already exists.</td>
<td>You attempted to create a proximity zone that is using an existing IP address.</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Region Error Messages

Table A-10 lists the potential error messages that may appear when configuring regions.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The region is still being referenced by other objects and cannot be removed.</td>
<td>You attempted to delete a region that is associated with GSSs on your GSS network.</td>
<td>Disassociate the GSSs from the region and then try again to delete the region.</td>
</tr>
<tr>
<td>There already exists a region named <code>&lt;region name&gt;</code>. All region names have to be unique.</td>
<td>You attempted to assign a name to the region that is already being used by another region on your GSS network.</td>
<td>Assign a unique name to your region.</td>
</tr>
</tbody>
</table>

## Source Address List Error Messages

Table A-11 lists the potential error messages that may appear when configuring source addresses.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid source address block '&lt;block string&gt;'. Address block must specify a host or a network.</td>
<td>You attempted to specify an invalid source address range.</td>
<td>Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.</td>
</tr>
<tr>
<td>Invalid source address block '&lt;blockstring&gt;'. Address block must specify a class A, B, or C host or network.</td>
<td>You attempted to specify an invalid source address range.</td>
<td>Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.</td>
</tr>
<tr>
<td>Invalid source address list name. Name must be entered.</td>
<td>You attempted to create a source address list without assigning a name to the list.</td>
<td>Enter a name for the source address list in the Name field.</td>
</tr>
<tr>
<td>Invalid source address list name. Name length must not exceed 80 characters.</td>
<td>You attempted to create a source address list with a name that is too long.</td>
<td>Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.</td>
</tr>
<tr>
<td>Invalid source address list name. Name must not contain spaces.</td>
<td>You attempted to create a source address list with a name that contains spaces. Source address list names cannot contain spaces.</td>
<td>Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.</td>
</tr>
<tr>
<td>This source address list cannot be deleted because it is referenced by &lt;number&gt; DNS rules.</td>
<td>You attempted to delete a source address list that is referenced by one or more DNS rules.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table A-11  Source Address List Error Messages (continued)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A source address list named '&lt;name&gt;' already exists. Name must uniquely identify a source address list.</td>
<td>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.</td>
<td>Assign a unique name to your source address list that is no more than 80 characters and does not contain spaces.</td>
</tr>
</tbody>
</table>

| 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. |

Table A-12  Sticky Error Messages

Table A-12 lists the potential error messages that may appear when configuring DNS sticky.

Table A-12  Sticky Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.</td>
<td>You entered an incorrect global subnet mask in the Global Proximity Configuration details page.</td>
<td>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).</td>
</tr>
</tbody>
</table>

| 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)

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Sticky inactivity timeout. Sticky inactivity timeout must be a multiple of 5.</td>
<td>You entered an incorrect Entry Inactivity Timeout value in either the Global Sticky Configuration details page or in the DNS Rules Builder.</td>
<td>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.</td>
</tr>
<tr>
<td>Invalid encryption string. Its length must not exceed 32 characters.</td>
<td>You entered an incorrect encryption string in the Global Sticky Configuration details page (Traffic Mgmt tab).</td>
<td>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.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Description</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Invalid view name. Name must be entered.</td>
<td>You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.</td>
<td>Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>Invalid view name. Name length must not exceed 80 characters.</td>
<td>You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.</td>
<td>Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>A view named [name] already exists. Name must uniquely identify a view.</td>
<td>You entered a duplicate view name in the Create User Views details page or the Modify User Views details page.</td>
<td>Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>The maximum number of 500 owners per view has been met.</td>
<td>The primary GSSM GUI supports a maximum of 500 owners in a custom user view.</td>
<td>If necessary, delete one or more owners previously assigned to the custom view. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>The maximum number of 1000 locations per view has been met.</td>
<td>The primary GSSM GUI supports a maximum of 1000 locations in a custom user view.</td>
<td>If necessary, delete one or more locations previously assigned to the custom view. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>The maximum number of 100 answers per view has been met.</td>
<td>The primary GSSM GUI supports a maximum of 100 answers in a custom user view.</td>
<td>If necessary, delete one or more answers previously assigned to the custom view. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
<tr>
<td>The maximum number of 100 keepalives per view has been met.</td>
<td>The primary GSSM GUI supports a maximum of 100 keepalives in a custom user view.</td>
<td>If necessary, delete one or more keepalives previously assigned to the custom view. See the Cisco Global Site Selector Administration Guide for details.</td>
</tr>
</tbody>
</table>
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
Appendix B  Sticky and Proximity XML Schema Files

Sticky XML Schema File Contents

The following example identifies the contents of the sticky XML schema, stickySchema.xsd:

```xml
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <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: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"/>  
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```
The following example identifies the contents of the proximity XML schema, proximitySchema.xsd:

```xml
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      Cisco GSS Proximity Database
    </xs:documentation>
  </xs:annotation>

  <xs:element name="ProximityDatabase" type="ProximityDatabaseType"/>
  <xs:element name="Header" type="HeaderType"/>
  <xs:element name="Entry" type="EntryType"/>
  <xs:element name="ProbeTarget" type="ProbeTargetType"/>
  <xs:element name="Zone" type="ZoneType"/>

  <xs:complexType name="ProximityDatabaseType">
    <xs:sequence>
      <xs:element ref="Header" minOccurs="1" maxOccurs="1"/>
      <xs:element ref="Entry" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="HeaderType">
    <xs:sequence>
      <xs:choice minOccurs="1" maxOccurs="1">
        <xs:element name="N" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="G" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
      </xs:choice>
      <xs:element name="D" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="R" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="A" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="H" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
      <xs:element name="T" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="EntryType">
    <xs:sequence>
      <xs:choice minOccurs="1" maxOccurs="1">
        <xs:element name="N" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="G" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
      </xs:choice>
      <xs:element name="D" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="R" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="A" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="H" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
      <xs:element name="T" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ProbeTargetType">
    <xs:sequence>
      <xs:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="Location" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ZoneType">
    <xs:sequence>
      <xs:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="Location" type="xsd:string" minOccurs="1" maxOccurs="1"/>
      <xs:element name="Priority" type="xsd:integer" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
<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>
</xsd:simpleType>

<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>
<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: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: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:schema>

<xsd:simpleType name="ZoneIdType">
    <xsd:restriction base="xsd:integer">
        <xsd:minInclusive value="1"/>
        <xsd:maxInclusive value="32"/></xsd:restriction>
    </xsd:simpleType>
</xsd:schema>
**A**

**Application Control Engine (ACE)**
Network device that performs high-performance server load balancing (SLB) among groups of servers, server farms, firewalls, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information. The ACE can also terminate and initiate SSL-encrypted traffic so that it can perform intelligent load balancing while ensuring secure end-to-end encryption. The ACE is available as a standalone appliance or as module for use in a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router.

**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 makes 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.
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.

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 proximity probing agents, 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 proximity probing agent in a zone. The GSS communicates with the Cisco IOS-based router using the DRP ICMP echo-based RTT query and response method.

**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 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.

**HTTPS 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 HTTPS HEAD keepalive type sends a TCP format HTTPS 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 an SLB device such as a CSS, CSM, or ACE. 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 an SLB device such as a CSS, CSM, or ACE. 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.
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.

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.
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.

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 proximity probing agents 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 proximity probing agent (DRP agent) to a requesting D-proxy device. Probe management is the intelligence behind each GSS device’s interaction with the proximity probing agent in a zone. Within each zone, there must be at least one proximity probing agent and, optionally, a backup proximity probing agent. If the primary proximity probing agent fails, the probes are redirected to the backup device. Once the primary proximity probing agent becomes available, probes are redirected back to the primary proximity probing agent. 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 proximity probing agent, 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.
### Glossary

**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 proximity probing agents in the GSS network, instructing the DRP agent in the proximity probing agent to probe specific D-proxy IP addresses. Each proximity probing agent 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 Kal**

Keepalive type used when the GSS answer that you are testing is a VIP associated with an SLB device such as a CSS, CSM, or ACE. The Scripted Kal keepalive type is used to probe third-party devices and obtain the load information. Scripted Kal 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 proximity probing agent is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one proximity probing agent to a requesting D-proxy device.
INDEX

A
answer
activating 1-39
associating with a proximity-based location 10-14
configuring 6-1
CRA-type answer, creating 6-10
CRA-type answer, overview 1-16
deleting 6-14
hit count 11-59
keepalive 1-16
keepalive statistics 11-59
modifying all in location 6-13
modifying an answer 6-12
monitoring 11-59
name server-type answer, creating 6-11
name server-type answer, overview 1-15
overview 1-14, 6-1
reactivating 6-13
setting all to ICMP 1-39
setting all to none 1-39
statistics, monitoring 11-3
status 11-60
suspension 1-39, 6-12
suspending all answers in a location 6-13
VIP-type answer, creating 6-2
VIP-type answer, multi-port 1-23, 6-4
VIP-type answer, overview 1-15

answer group
adding answers 6-16
balance method options 1-25
balance methods 6-14
CRA configuration information 7-13
creating 6-15
deleting 6-20
DNS rule 1-12, 1-14, 6-1
DNS Rule Wizard 7-6
error messages A-3
general configuration 6-16
load threshold 6-16
modifying 6-17
order 6-16
overview 1-14, 6-14
removing answers 6-17
statistics, monitoring 11-4
suspension 6-19
suspending or reactivating all for an owner 6-19
weight 6-16
answer hit counts 11-58
answer keepalive statistics 11-59
Anywhere source address 1-13, 3-1
appliance-based global server load balancing 1-7
Application Control Engine
data center deployment 1-33
definition G-1
global load-balancing 1-2
network deployment 1-7
A record 7-9, 7-11
attacks command 11-12

B
balance clause 6-14, 7-11, 9-13, 10-19
balance method
answer group options 1-25
answer group pair 6-14
balance clauses 6-14
boomerang 1-25
DNS rule 1-12, 1-14, 6-1
DNS Rule Wizard 7-8
hash 1-25, 7-8, 7-11
hashed balance method 7-11
least loaded 1-24, 7-11
load threshold option 7-7
ordered list 1-24, 7-8, 7-11, 7-12
order option 1-26, 7-7
overview 1-23
proximity 10-18
round robin 1-24, 7-8, 7-11, 7-12
sticky 9-12
weighted round robin 1-24, 7-9, 7-11, 7-12
weight option 1-26, 7-7
BIND sample zone configuration file 7-23
boomerang
activity, monitoring 11-2
balance method 1-25
clear statistics 11-57
DNS race 1-25
server 1-25
server, monitoring status 11-2
server status 11-2
browsers supported 1-35

closeness (DNS race) 6-10
communication between nodes 1-33
Content Services Switch
data center deployment 1-33
definition G-2
global load-balancing 1-2
GSS network deployment 1-7
VIP answers 1-15
Content Switching Module
data center deployment 1-33
definition G-2
global load-balancing 1-2
GSS network deployment 1-7
VIP answers 1-15
CRA
answer, creating 6-10
balance method 1-26, 6-14
clear statistics 11-57
closeness 6-10
CRA answer overview 1-16
definition G-2
DNS race 6-10
global keepalive configuration 5-8
keepalive 1-20
last gasp address 7-9
minimum frequency 5-9
one way delay 6-11
overview 1-20
proximity DNS race 6-10
round-trip time 6-11
showing statistics 11-19
Create icon 1-37
CSM
See Content Switching Module
CSS
See Content Services Switch

C
Cancel icon 1-38
CIDR block masking 3-1
Cisco IOS-based router
DRP agent, configuring 10-10
IOS release 12.1 interoperability considerations 10-11
selecting as DRP agent 10-10
supported releases 10-10
clauses (balance clause) in answer group 6-14
CLI device management 1-34
data center
  definition 6-2
  deployment 1-33

DDoS
  attacks statistics, clearing 11-57
  attack statistics, displaying 11-12
  clear statistics 11-57
  detection and mitigation
    affected network areas 1-29
    anti-spoofing 1-31
    configuration 1-29
    filter checking 1-30
    overview 1-29
    rate-limiting 1-30
    types of attacks prevented 1-29
  failed DNS queries, displaying 11-14
  global statistics, clearing 11-57
  global statistics, displaying 11-17
  rate-limits, displaying 11-15
  running configuration, displaying 11-16, 11-19
  spoofed/non-spoofed D-proxies, displaying 11-13
  statistics, monitoring 11-63
  show 11-12, 11-13, 11-14, 11-15, 11-17, 11-19

delegation
  definition 1-2
  domains to GSS 1-32, 7-22
  GSS devices 7-22
  subdomains to GSS 1-32, 7-22

Delete icon 1-38

deployment
  configuring name servers 7-22
  data center 1-33
  locations and regions 2-2
  overview 1-32
  resources 2-2
  typical GSS deployment 1-32

details pages 1-36

DNS
  all 7-9, 7-10
  A record 7-9, 7-11
  balance clause 7-11, 9-13, 10-19
  clear statistics 11-57
  creating DNS rules 7-3
  delegation 7-22
  DNS queries 7-9, 7-10
  glue A records 7-22
  hosted domain 1-14
  iterative request 1-6
  negative response queries 1-4
    common response codes 1-4
    query 1-13
    race 1-16, 6-10
    record request 7-9, 7-10
    recursive request 1-5
    request resolution 1-6
    resource records 1-3
    routing overview 1-2
    sample BIND zone configuration 7-23
    server, modifying 7-22
    server, monitoring 11-2
    SOA records 1-4
      configuring for negative responses 1-5
        fields 1-4
        format 1-4
        TTL 1-4
        TTL fields 1-4
        traditional routing 1-2
        unmatched queries 11-62
    zone configuration file 7-22

DNS race
  balance method 1-25
  closeness 6-10
  coordinate start time 6-10
  CRAs 1-16

DNS rule
  activating 1-39
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>answer</strong> 1-12, G-1</td>
</tr>
<tr>
<td><strong>balance clause</strong> 6-14</td>
</tr>
<tr>
<td><strong>components</strong> 1-12</td>
</tr>
<tr>
<td><strong>creating</strong> 7-2, 8-4</td>
</tr>
<tr>
<td><strong>definition</strong> G-2</td>
</tr>
<tr>
<td><strong>deleting</strong> 7-17</td>
</tr>
<tr>
<td><strong>error messages</strong> A-5</td>
</tr>
<tr>
<td><strong>filtering</strong> 1-38</td>
</tr>
<tr>
<td><strong>filters, configuring</strong> 7-18</td>
</tr>
<tr>
<td><strong>filters, removing</strong> 7-22</td>
</tr>
<tr>
<td><strong>hit count</strong> 11-61</td>
</tr>
<tr>
<td><strong>modifying</strong> 7-14</td>
</tr>
<tr>
<td><strong>overview</strong> 1-12</td>
</tr>
<tr>
<td><strong>proximity, enabling/disabling</strong> 10-19</td>
</tr>
<tr>
<td><strong>reactivating</strong> 7-16</td>
</tr>
<tr>
<td><strong>reactivating all by owner</strong> 7-17</td>
</tr>
<tr>
<td><strong>removing filters</strong> 7-22</td>
</tr>
<tr>
<td><strong>showing all rules</strong> 1-38</td>
</tr>
<tr>
<td><strong>statistics, monitoring</strong> 11-8</td>
</tr>
<tr>
<td><strong>sticky, disabling</strong> 9-13</td>
</tr>
<tr>
<td><strong>sticky, enabling by domain</strong> 9-13</td>
</tr>
<tr>
<td><strong>sticky, enabling by domain list</strong> 9-13</td>
</tr>
<tr>
<td><strong>sticky, enabling for balance clause</strong> 9-14</td>
</tr>
<tr>
<td><strong>sticky inactivity timeout</strong> 9-13</td>
</tr>
<tr>
<td><strong>sticky overview</strong> 9-12</td>
</tr>
<tr>
<td><strong>suspending</strong> 1-39, 7-15</td>
</tr>
<tr>
<td><strong>suspending all by owner</strong> 7-17</td>
</tr>
<tr>
<td><strong>DNS Rule Builder</strong></td>
</tr>
<tr>
<td><strong>balance clause</strong> 7-11, 9-13, 10-19</td>
</tr>
<tr>
<td><strong>CRA configuration information</strong> 7-13</td>
</tr>
<tr>
<td><strong>creating DNS rules</strong> 7-10</td>
</tr>
<tr>
<td><strong>DNS queries</strong> 7-10</td>
</tr>
<tr>
<td><strong>modifying DNS rule</strong> 7-14</td>
</tr>
<tr>
<td><strong>name server balance methods</strong> 7-8, 7-11</td>
</tr>
<tr>
<td><strong>overview</strong> 7-2</td>
</tr>
<tr>
<td><strong>proximity, enabling</strong> 10-19</td>
</tr>
<tr>
<td><strong>sticky, enabling</strong> 9-13</td>
</tr>
<tr>
<td><strong>VIP balance methods</strong> 7-11</td>
</tr>
<tr>
<td><strong>DNS rule filter</strong></td>
</tr>
</tbody>
</table>
hit counts 11-61
maximum length 4-2, 7-5
maximum name length 4-2, 7-5
maximum per domain list 1-14, 4-1
statistics, monitoring 11-5
sticky by domain 9-13
wildcards maximum length 4-2, 7-5

D-proxy
background 1-5
definition G-3
iterative requests 1-6
name server forwarding 1-15
query GSS 1-13
dproxy command 11-13

DRP
authentication, enabling (Cisco IOS router) 10-10
authentication, enabling (GSS) 10-17
key chain (Cisco IOS router) 10-10
key identification number (GSS) 10-17
keys, creating (Cisco IOS router) 10-10
keys, creating (GSS) 10-17
keys, deleting (GSS) 10-18
key string number (GSS) 10-18
overview 10-2

DRP agent
clear statistics 11-57
configuring Cisco IOS-based router 10-10
displaying status 11-11
enabling 10-10
IOS release 12.1 interoperability considerations 10-11
overview 10-2
RTT measurement 10-2
selecting Cisco IOS-based router 10-10
supported Cisco IOS releases 10-10
drpagent
activity, displaying 11-11
server status 11-11

E
error messages
answer group A-3
DNS rule A-5
domain list A-11
GSSM A-17
location A-13
owner A-13
proximity A-14
region A-14
shared keepalive A-11
source address list A-17
sticky A-18
user A-19
user view A-19
user views A-19
exporting icon 1-37
Export to CSV icon 1-37

F
failed-dns command 11-14
failure detection time, adjusting 1-21
filters
DNS rules 7-18
parameters 7-18, 7-19, 7-20
removing 7-22
firewall
deploying GSS devices 1-32
permitting traffic to GSS 1-33
fully qualified domain name G-3, G-4

G
GeoDB Configuration 8-4
GeoDB Static Entries 8-5
GeoDB Statistics 8-6
GeoIP database (GeoDB) 8-1
global keepalives
  CRA configuration settings 5-8
  fast transmission rate 1-21
  HTTP HEAD configuration settings 5-4
  ICMP configuration settings 5-2
  KAL-AP configuration settings 5-7
  modifying 5-1
  name server configuration settings 5-9
  overview 5-1
  properties, modifying 5-1
  Scripted keepalive configuration settings 5-8
  standard transmission rate 1-21
  TCP configuration settings 5-3

global manual reactivation 2-8

global server load balancing
  balance clauses 6-14
  configuration order 1-40
  data centers 1-33
  definition 6-3
  delegation of GSS devices 7-22
  global statistics 11-62
  monitoring 11-58
  overview 1-7
  summary 1-40
  traffic management overview 1-27
  using the GSS 1-7

Global Site Selector
  acting as GSSM 1-10, 1-32
  authoritative DNS server 1-7
  balancing data centers 1-33
  boomerang server 11-2
  CLI-based management 1-34
  communication 1-33
  delegation of devices 7-22
  deployment 1-32, 1-33, 7-22
  DNS server, monitoring 11-2
  factors in responding to a request 1-7
  general statistics, monitoring 11-6
  global server load balancing 1-7

  GSLB configuration 1-40
  GUI-based management 1-34
  hardware 1-10, 1-11
  interact with SLBs 1-7
  inter-GSS communications 1-33
  keepalives overview 1-16, 5-1
  locating 1-32
  network management 1-34
  overview 1-2, 1-11
  packet filtering 1-33
  resources, grouping 2-7
  software architecture 1-10
  synchronized with GSSM 1-11, 1-33

Global Site Selector Manager
  communication 1-33
  database 1-10, 1-33
  definition G-3
  deployment 1-32
  DNS rule configuration interface 7-2
  DNS rules 1-12
  error messages A-17
  GSLB configuration 1-40
  GUI overview 1-35
  icons 1-37
  inter-GSS communication 1-33
  keepalives overview 5-1
  locating 1-32
  online help 1-39
  overview 1-10
  primary 1-10
  primary GSSM GUI overview 1-35
  redundancy 1-33
  resources, grouping 2-7
  standby 1-11
  standby, as backup 1-32
  standby acting as primary 1-33
  global statistics 11-65
  global sticky
  authentication 9-4, 9-11
by domain, enabling  9-13
by domain list, enabling  9-13
clearing sticky mesh statistics  11-57
enabling from GUI  9-10
encryption  9-4, 9-11
favored peer  9-6, 9-11
joining the mesh  9-5
mesh, communicating  9-5
mesh configuration  9-11
mesh conflict resolution  9-5
mesh statistics  11-42, 11-51
mesh updates  9-4
messaging statistics  11-38, 11-47, 11-48
overview  9-3
peer mesh  9-4
synchronizing GSS system clock with peers  9-8
glossary of terms  G-1
glue A records  7-22
GSLB
   See global server load balancing
GSS
   See Global Site Selector
GSSM
   See Global Site Selector Manager
GSS network
   configuration  1-10, 1-33
definition  G-3
deployment  1-32
global statistics  11-62, 11-65
GSLB status  11-58
management  1-34
monitoring through CLI  11-1
monitoring through GUI  11-58
organizing  2-2
primary GSSM  1-10
resource grouping  2-7
GUI
   browsers supported  1-35
details pages  1-36
device management  1-34
error messages  A-1
icons  1-37
list pages  1-36
logging on  1-35
monitoring GSS device status  11-30
navigation  1-37
organization  1-36
overview  1-35
refreshing  1-38
tsaps  1-36
understanding  1-35
GUI error messages  A-1
hashed balance method  1-25, 7-8, 7-11
help
   navigation link  1-39
   obtaining  1-39
   primary GSSM Online help overview  1-39
hosted domain
   definition  G-4
domain names  1-14
name examples  1-14
overview  1-14, 4-1
regular expressions  1-14
requested  1-12
statistics  11-61
HTTP HEAD keepalive
   default path  5-5, 5-12, 6-7
destination port  5-4, 5-6, 6-7, 6-8
global keepalive configuration  5-4
host tag  5-12, 6-7
overview  1-19
shared keepalive configuration  5-12, 5-13
statistics  11-23, 11-24
termination method  5-5, 5-12, 6-7
VIP answer  6-7, 6-8
ICMP keepalive
  global keepalive configuration 5-2
  overview 1-18
  shared keepalive configuration 5-10, 5-15
  statistics 11-25
  VIP answer 6-5, 6-9

icons 1-37

inter-GSS communication 1-33

iterative requests 1-6

K

KAL
  See keepalive
KAL-AP keepalive
  by tag 6-9
    CAPP hash secret 5-7, 5-14
    global keepalive configuration 5-7
    overview 1-19
    shared keepalive configuration 5-14
    statistics 11-26
    VIP answer 6-9

keepalive 6-2
  clear statistics 11-57
  cra, clear statistics 11-57
  CRA overview 1-20
  CRA statistics, monitoring 11-19
  CRA type 1-20
  definition 6-4
  deleting a shared keepalive 5-17
  error messages A-11
  failure detection time, adjusting 1-21
  fast transmission rate 1-21
  global properties, modifying 5-1
  global properties, overview 5-1
  global statistics, monitoring 11-20
  http-head, clear statistics 11-57

HTTP HEAD connection termination method 5-5, 5-12, 6-7
HTTP HEAD overview 1-19
HTTP HEAD statistics, monitoring 11-23, 11-24
https-head, clear statistics 11-57
ICMP statistics, monitoring 11-25
ICMP type 1-18
kalap, clear statistics 11-57
KAL-AP overview 1-19
KAL-AP statistics, monitoring 11-26
keepalive attempts 1-23, 5-11, 5-13, 5-14, 5-16, 6-6, 6-7
multi-port 1-17
name server 1-20
name server overview 1-20
name server statistics, monitoring 11-28
none 1-20
ns, clear statistics 11-57
number of retries 1-22, 5-3, 5-4, 5-5, 5-7, 5-8, 5-11, 5-12, 5-14, 6-5, 6-6, 6-7
overview 1-16
probes 1-23, 5-11, 5-13, 5-14, 5-16, 6-6, 6-7
scripted-kal, clear statistics 11-57
Scripted keepalive overview 1-20
Scripted statistics, displaying 11-27
shared keepalive, creating 5-9
shared keepalive, modifying 5-17
shared keepalive overview 5-9
shared VIP keepalives, overview 5-9
standard transmission rate 1-21
supported types 1-17
TCP connection termination method 5-3, 5-11, 6-6
TCP overview 1-19
TCP statistics, monitoring 11-29
transmission interval formula 11-29
VIP 1-18, 1-19, 5-9

L

last gasp address 7-9
least loaded 7-11
  balance method 1-24, 7-8, 7-11
  overview 1-24, 7-8, 7-11
  weight option 1-26
list pages
  overview 1-36
  sorting items 1-36
load threshold, balance method option 7-7
local sticky
  disabling on a GSS 9-21
  enabling from GUI 9-10
  enabling on a GSS 9-21
  overview 9-2
location
  associating with a proximity zone 10-13
  creating 2-4
  definition G-5
  deleting 2-5
  error messages A-13
  modify all answers in 6-13
  modifying 2-5
  organizing resources 2-7
  overview 1-12, 2-2
  suspending all answers 6-13

M
  manual reactivation
    global 2-8
  manual reactivation option
    clauses 7-12, 7-13
    CRA answers 6-10
    name server answers 6-11
    VIP answers 6-3
Modify icon 1-37
monitoring
  answer hit counts 11-58
  answer keepalive statistics 11-59
  answer status 11-60
boomerang server status 11-2
DNS rule statistics 11-61
DNS server 11-2
global load-balancing status 11-58
global statistics 11-65
global sticky mesh statistics 11-42, 11-51
global sticky messaging statistics 11-38, 11-47, 11-48
GSS network status through CLI 11-1
hosted domain statistics 11-61
proximity database statistics 11-31, 11-36, 11-66
proximity DNS rule hit count statistics 11-65
proximity group configuration 11-35, 11-36
proximity group statistics 11-32
proximity lookup statistics 11-8, 11-30, 11-33, 11-66
proximity group statistics 11-33, 11-34, 11-67
proximity probe statistics 11-33, 11-34, 11-67
proximity status 11-35
source address statistics 11-62
status of GSS devices from the GUI 11-30
sticky database statistics 11-38, 11-46, 11-68
sticky DNS rule hit count statistics 11-67
sticky global mesh statistics 11-68
sticky group statistics 11-44, 11-56
sticky lookup statistics 11-11, 11-37
sticky status 11-45

Monitoring tab 1-36

N
  name server
    answer type, creating 6-11
    authoritative 1-6
    authoritative name server (ANS) 1-5
    balance method 6-14
    balance method options 1-26
    balance methods 7-8, 7-11
    clear statistics 11-57
    client name server (CNS) 1-5
definition G-5
    DNS resolvers (DNSR) 1-5
Index

forwarding  1-15
intermediate name server (INS)  1-5
keepalive  1-20
name server answer overview  1-15
overview  1-5
query  6-12
records, adding to zone configuration file  7-22
root name servers (RNS)  1-5
name server keepalive
  global keepalive configuration  5-9
  minimum frequency  5-9
  overview  1-20
  query domain  5-9
  statistics  11-28
navigation through the GUI  1-37
negative DNS response queries  1-4
  common response codes  1-4
negative DNS responses queries SOA configuration  1-5
network
  deployment  1-32
  locating GSS on  1-32
network design guidelines for proximity  10-6
network management  1-34
  CLI-based  1-34
  GUI-based  1-34
  monitoring global server load-balancing statistics  11-58
network proximity
  See proximity
node communication  1-33
NTP server
  enabling  9-8, 10-11
  identifying  9-8, 10-11
  synchronizing GSS system clock with peers  9-8, 10-11
number of retries for keepalive types  1-22, 5-3, 5-4, 5-5, 5-7, 5-8, 5-11, 5-12, 5-14, 6-5, 6-6, 6-7

O
one-way delay  6-11
Online help overview  1-39
ordered list  7-11
  balance method  1-24, 7-8, 7-12
  definition  G-6
  overview  1-24
order option, balance method  1-26, 7-7
origin server  G-6
owner
  creating  2-6
  deleting  2-7
  error messages  A-13
  modifying  2-6
  organizing resources  2-7
  overview  1-13, 2-2
reactivating all DNS rules  7-17
suspending all answer groups for  6-19
suspending all DNS rules  7-17

P
PDB
  See proximity database
Print icon  1-37
proximity
  Acceptable RTT value  10-16, 10-19
  Acceptable Zone value  10-16, 10-19
  balance clause information  10-19
  clearing statistics  11-57
  configuring from CLI  10-20
  configuring from GUI  10-14
  database statistics, monitoring  11-31, 11-36, 11-66
delating database entries  10-25
delating static entries  10-25
disabling  10-14
DNS Rule Builder, adding to  10-19
DNS rule hit count statistics, monitoring  11-65
Index

DNS rule overview 10-18
DNS rule statistics, monitoring 11-8, 11-30
DRP authentication, enabling/disabling 10-17
dumping proximity database entries enabling 10-14, 10-19
Equivalence Window 10-15
error messages A-14, A-19
group configuration, monitoring 11-35, 11-36
group statistics, monitoring 11-32
inactivity timeout 10-5, 10-15
initial probe method 10-15
loading proximity database entries 10-28
locally disabling/enabling proximity on a GSS 10-30
lookup statistics, monitoring 11-33, 11-66
manually initiating probing 10-29
mask, specifying 10-15
network design guidelines 10-6
network proximity example overview 10-2
periodic proximity database backup 10-28
probe management overview 10-2
probe methods 10-4
probe statistics, monitoring 11-33, 11-34, 11-67
proximity database overview 10-4
proximity group, creating 10-22
proximity group deletion 10-23
proximity group overview 10-21
quick start 10-7
results of locally disabling on a GSS 10-30
static database entries, adding 10-23
statistics, monitoring (CLI) 11-30
statistics, monitoring (GUI) 11-65
status, monitoring (CLI) 11-30
subsystem statistics, monitoring 11-35
synchronizing GSS system clock with peers 10-11
wait-state condition, enabling/disabling 10-17, 10-20
XML schema file B-1
zone overview 10-2
zones, associating with a location 10-13
zones, associating with an answer 10-14
zones, creating 10-12
zones, deleting 10-13
zones, modifying 10-13
proximity database
age-out process 10-5
automatic backup 10-26
deleting dynamic entries 10-25
deleting static entries 10-25
dumping entries 10-26
inactivity timeout 10-5, 10-15
loading entries 10-28
maximum number of entries 10-5
overview 10-4
periodic backup 10-28
RTT, assigning to static entries 10-24
RTT values 10-4
specifying entry format to dump static entries, adding 10-23
proximity group
benefits 10-21
creating 10-22
deleting 10-23
entering multiple groups 10-23
IP address block, deleting 10-23
overview 10-21
proximity probing agent
assigning to static database entries 10-24
initial probe method 10-15
manually initiating probing 10-29
probe agent overview 10-2
probe methods 10-4
probing process 10-3
refresh probe interval 10-15
RTT results 10-4
proximity zone
Acceptable Zone value 10-16, 10-19
associating with a location 10-13
associating with an answer 10-14
creating 10-12
deleting 10-13
determining most proximate answer 10-4
Equivalence Window 10-15
modifying 10-13
network design guidelines 10-6
overview 10-2
probe methods 10-4
RTT 10-2

Q

query answers 6-1
balance methods 1-23
CRA answer 6-10
DNS request 1-6
DNS rules 1-12
KAL-AP 1-19, 6-9
match DNS query type 7-9
name server 1-20, 5-9
name server answer 6-11
not matched to D-proxy 1-13
query domain 5-9
source addresses 1-13
VIP answer 6-2

R

rate-limit command 11-15
reactivating
    all answer groups for an owner 6-19
    all answers in an answer group 6-19
    all answers in location 6-13
    all DNS rules by owner 7-17
    answer 6-13
    DNS rule 7-16
    record request 7-9
redundancy synchronization 1-33
Refresh icon 1-38
refreshing the GUI 1-38
region
    creating 2-2
    definition G-6, G-7
deleting 2-5
error messages A-14
modifying 2-3
organizing resources 2-7
overview 1-12, 2-2
regular expressions 1-14, 4-1, 4-2, 7-5
report
    answer hit counts 11-58
    answer status 11-60
    DNS rule hit count 11-61
domain hit count 11-61
    keepalive statistics 11-59
    source address hit count 11-63
requests
    iterative 1-6
    resolution 1-5, 1-7
resource records 1-3
resources
    configuring 2-1
    grouping 2-7
    organizing 2-2
Resources tab 1-36
round robin 7-11
    balance method 1-24, 7-8, 7-12
    overview 1-24
round-trip time (RTT)
    Acceptable RTT value 10-16, 10-19
    Acceptable Zone value 10-16, 10-19
assigning to static entries 10-24
    DRP agent 10-2
    Equivalence Window 10-15
    one-way delay (CRA) 6-11
    overview 10-2
Index

probing methods 10-4
proximity database entries 10-4
refresh probe interval 10-15

RTT
See round-trip time (RTT)
running-config command 11-19

dns sticky rule 11-11, 11-37
dpragent 11-11
keepalive 11-19
keepalive cra 11-19
keepalive global 11-20
keepalive http-head 11-23, 11-24
keepalive icmp 11-25
keepalive kalap 11-26
keepalive ns 11-28
keepalive tcp 11-29
proximity database 11-31
proximity group-name 11-32
proximity group-summary 11-32
proximity lookup 11-33
proximity probe 11-33, 11-34
scripted keepalive 11-27
source-address 11-10
source-address-list 11-10
sticky 11-38
sticky global 11-38
sticky group-name 11-44
sticky group-summary 11-44
sticky mesh 11-42

SOA records 1-4
configuring for negative responses 1-5
format 1-4
TTL fields 1-4

sort
DNS rules 7-18
removing 7-22

Sort icon 1-37

source address
Anywhere 1-13, 3-1
blocks 1-13, 3-1
hit counts 11-62
maximum per source address list 3-1
overview 1-13

statistics, monitoring 11-10

sample BIND zone configuration 7-23
scripted-kal
   clear statistics 11-57
Scripted keepalive
   global keepalive configuration 5-8
   overview 1-20
   statistics 11-27
server load balancer 1-2, G-7
service provider G-7
shared keepalive
   creating 5-9
   deleting 5-17
   error messages A-11
HTTP HEAD configuration settings 5-12, 5-13
ICMP configuration settings 5-10, 5-15
KAL-AP configuration settings 5-14
modifying 5-17
   overview 5-9
TCP configuration settings 5-11
show ddos-config command 11-16
show statistics command 11-1
boomerang 11-2
dns 11-2
dns answer 11-3
dns answer group 11-4
dns domain 11-5
dns domain-list 11-6
dns global 11-6
dns proximity rule 11-8, 11-30
dns rule 11-8
source address and domain hash balance method  1-25, 7-8, 7-11
source address list
    anywhere  1-13
    Anywhere (default)  3-1
    creating  3-1, 3-2
    definition  G-7
    deleting  3-3
error messages  A-17
general configuration  3-2
maximum addresses  3-1
modifying  3-3
overview  1-13
removing addresses  3-3
statistics, monitoring  11-10
SSL
    See Secure Socket Layer
standby GSSM
    database, synchronized with primary GSSM  1-33
definition  1-33
overview  1-11
statistics
    answer hit counts  11-58
    answer keepalive  11-59
    answer status  11-60
clearing  11-57
    clearing DDoS  11-57
    DNS rule hit count  11-61
global  11-65
    hosted domains  11-61
    proximity database  11-66
    proximity DNS rule hit count  11-65
    proximity lookup  11-66
    proximity probe  11-67
    source address  11-62
sticky database  11-46, 11-68
sticky DNS rule hit count  11-67
sticky global mesh  11-68
traffic management, monitoring  11-65
statistics-global command  11-17
sticky
    balance clause, enabling for  9-14
    by domain, enabling  9-13
    by domain list, enabling  9-13
clearing statistics  11-57
configuring from CLI  9-14
configuring from GUI  9-9
disabling  9-10, 9-13
disabling/enabling local sticky on a GSS  9-21
DNS Rule Builder, adding to  9-13
DNS rule hit count statistics, monitoring  11-67
DNS rule overview  9-12
DNS rule statistics, monitoring  11-11, 11-37
dumping sticky database entries  9-19, B-1
devices    9-20
downstream devices  9-20
equivalent domain list  9-13
error messages  A-18
    global sticky mesh authentication  9-11
    global sticky mesh configuration  9-11
    global sticky mesh encryption  9-11
    global sticky mesh statistics, monitoring  11-42, 11-51
global sticky mesh messaging statistics, monitoring  11-38, 11-47, 11-48
global sticky overview  9-3
global sticky peer mesh  9-4
    group statistics, monitoring  11-44, 11-56
    inactivity timeout  9-3, 9-10, 9-13
    loading sticky database entries  9-21
    local sticky overview  9-2
    mask, specifying  9-10
    mesh favored peer  9-6, 9-11
    overview  9-1
periodic sticky database backup  9-20
quick start guide  9-6
results of locally disabling on a GSS  9-21
statistics, monitoring (CLI)  11-37
statistics, monitoring (GUI)  11-65
status, monitoring (CLI) 11-37
sticky database overview 9-2
sticky global mesh statistics, monitoring 11-68
sticky group, creating 9-17
sticky group, deleting 9-17
sticky group deletion 9-18
sticky group overview 9-15
subsystem statistics, monitoring 11-45
XML schema file B-1
sticky database
age-out process 9-3
automatic backup 9-19
dumping entries 9-19
loading entries 9-21
matched entry 9-3
maximum number of entries 9-3
overview 9-2
periodic backup 9-20
specifying entry format to dump 9-19, B-1
statistics 11-46
sticky entries, deleting 9-18
sticky inactivity timeout 9-3, 9-10, 9-13
sticky group
creating 9-17
deleting 9-18
entering multiple groups 9-17
IP address block, deleting 9-17
overview 9-15
subdomains, delegation 1-32, 7-22
Submit icon 1-38
subscriber G-8
suspending
all answer groups for an owner 6-19
all answers in a location 6-13
all answers in an answer group 6-19
all DNS rules by owner 7-17
answer 6-12
answer group 6-19
DNS rule 7-15
synchronization of primary and standby GSSM 1-33
TCP keepalive
destination port 5-3, 6-6
global keepalive configuration 5-3
overview 1-19
shared keepalive configuration 5-11
statistics 11-29
termination method 5-3, 5-11, 6-6
VIP answer 6-6
Time To Live G-8, G-9
Tools tab 1-36
traffic management
load balancing overview 1-27
proximity, configuring 10-14
proximity overview 1-28
proximity zone, configuring 10-12
statistics, monitoring 11-65
sticky, configuring 9-9
sticky overview 1-27
Traffic Mgmt tab 1-36
troubleshooting GUI error messages A-1
TTL
See Time To Live
user interface
details windows 1-36
icons 1-37
list windows 1-36
navigation 1-37
organization 1-36
understanding 1-35
user view error messages A-19
Index

V

VIP
   answer groups 6-14
   answers 6-2
   balance method options 1-26
   balance methods 6-14, 7-8, 7-11
   http-head, clear statistics 11-57
   https-head, clear statistics 11-57
   icmp, clear statistics 11-57
   kal-ap, clear statistics 11-57
   keepalive type 1-18
   tcp, clear statistics 11-57
   VIP answer overview 1-15

VIP answer
   answer types 6-4
   creating 6-2
   HTTP HEAD keepalive 6-7, 6-8
   ICMP keepalive 6-5, 6-9
   KAL-AP keepalive 6-9
   multiple answers and ports, specifying 1-23, 6-4
   multi-port 1-17, 6-2
   TCP keepalive 6-6

VIP keepalive type
   HTTP HEAD 1-19
   ICMP 1-18
   KAL-AP 1-19
   Scripted keepalive 1-20
   TCP 1-19

VIP-type answer, multi-port 1-17, 1-39, 6-2

W

weight
   balance method overview 1-26, 7-7
   least loaded 1-26
   round-robin 1-26

weighted round robin
   balance method 1-24, 7-9, 7-12