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

Software Version 2.0
March 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-10412-01

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

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

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

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

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

© 2007 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 5

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, Obtaining Support, and Security Guidelines

Audience

To use this configuration guide, you should be familiar with the GSS platform hardware. In addition, you should be familiar with basic TCP/IP and networking concepts, router configuration, Domain Name System (DNS), theBerkeley Internet Name Domain (BIND) software or similar DNS products, and your organization's specific network configuration.

How to Use This Guide

This guide includes the following chapters:

Chapter/Title	Description
Chapter 1, Introducing the Global Site Selector	Describes the basic concepts underlying the GSS product as well as important GSS-related terms.
Chapter 2, Configuring Resources	Instructions on organizing resources on your GSS network as locations, regions, and owners.
Chapter 3, Configuring Source Address Lists	Describes the creation and modification of source address lists.
Chapter 4, Configuring Domain Lists	Describes the creation and modification of domain lists.
Chapter 5, Configuring Keepalives	Describes the modification of global keepalive parameters and the creation of shared keepalives.
Chapter 6, Configuring Answers and Answer Groups	Describes the creation of GSS answers and answer groups.
Chapter 7, Building and Modifying DNS Rules	Describes how to construct the DNS rules that govern all global server load balancing on your GSS network.
Chapter 8, Configuring DNS Sticky	Describes how to configure local and global DNS sticky for GSS devices in your network.
Chapter 9, Configuring Network Proximity	Describes how to configure proximity for GSS devices in your network.

Chapter/Title	Description
Chapter 10, Monitoring GSS Global Server Load-Balancing Operation	Describes the tools that you can use to monitor the status of global load balancing on your GSS network.
Appendix A, Primary GSSM Global Server Load-Balancing Error Messages	Describes the primary GSSM global server load-balancing operating error messages.
Appendix B, Sticky and Proximity XML Schema Files	Describes how you can use the two XML schema files, included with the GSS, to describe and validate the sticky XML and proximity XML output files.

Related Documentation

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

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

Document Title	Description
Cisco Global Site Selector Administration Guide	Provides the procedures necessary to properly set up, manage, and maintain your GSSM and GSS devices, including login security, software upgrades, GSSM database administration, and logging.
Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide	Includes information on configuring the primary GSSM from the CLI to perform global server load balancing.
Cisco Global Site Selector Command Reference	Provides an alphabetical list of all GSS command-line interface (CLI) commands including syntax, options, and related commands. This document also describes how to use the CLI interface.

Symbols and Conventions

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

Command descriptions use the following conventions:

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

Screen examples use the following conventions:

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

Graphical user interface elements use the following conventions:

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

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

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

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

CHAPTER 1

Introducing the Global Site Selector

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

This chapter contains the following major sections:

- GSS Overview
- DNS Routing
- GSS as a DNS Appliance
- 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

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

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

GSS Overview

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

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

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

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

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

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

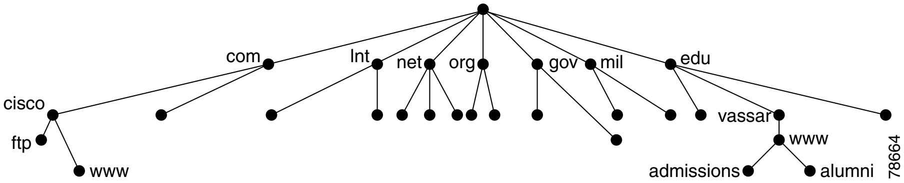
DNS Routing

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

Since the early 1980s, content routing on the Internet has been handled using the Domain Name System (DNS), a distributed database of host information that maps domain names to IP addresses. Almost all transactions that occur across the Internet rely on DNS, including electronic mail, remote terminal access such as Telnet, file transfers using 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 *(*Figure 1-1). DNS allows local administration of segments (individual domains) of the overall database, but allows for data in any segment to be available across the entire network. This process is referred to as *delegation*.

Figure 1-1 Domain Name Space



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 supported record types, as well as instructions for configuring resource records, see the *Cisco CNS Network Registrar User's Guide*. You can also consult RFC 1034 and 1035 for additional background information on resource records.

This section contains the following topics:

- SOA Records
- Negative Caching
- SOA Records and Negative Responses

SOA Records

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

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

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

Negative Caching

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

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

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

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

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

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

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

SOA Records and Negative Responses

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

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

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

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

To configure SOA records on the GSS to use in the negative response, you need to configure an NS answer that specifies the IP address of the authority name server for the domain and the domains hosted on the name server. See the "Configuring an Authority Domain for an Answer Group" section in Chapter 6, for more details.

IDNS 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:

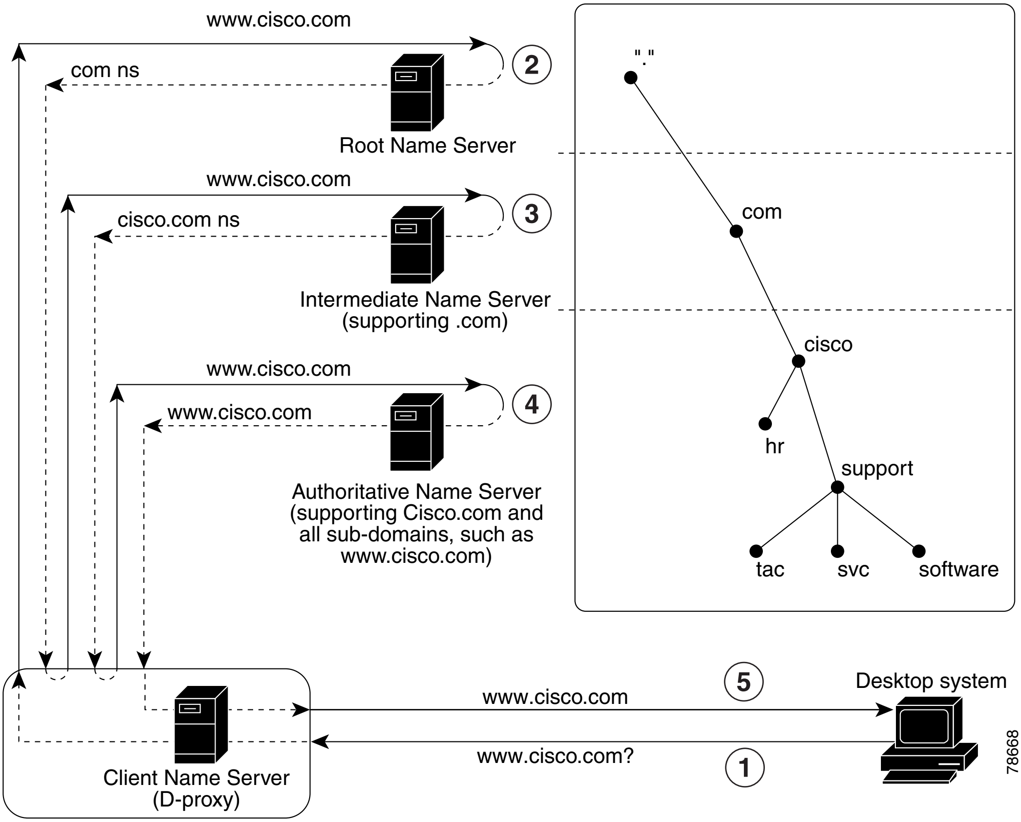
- DNS Resolvers—Clients that access client name servers.
- Client Name Server—Server that runs DNS software that has the responsibility of finding the requested web site. The client name server is also referred to as the client DNS proxy (D-proxy).
- Root Name Servers—Server that resides at the top of 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 sever is authoritative for the requested domain and sends the IP address to the name server (D-proxy).
5. The name server (D-proxy) sends the IP address (172.16.56.76) to the client browser. The browser uses this IP address and initiates a connection to the www.cisco.com website.

GSS as a DNS Appliance

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

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

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

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

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

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

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

Globally Load Balancing with the GSS

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

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

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

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

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

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

This type of global server load balancing 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.

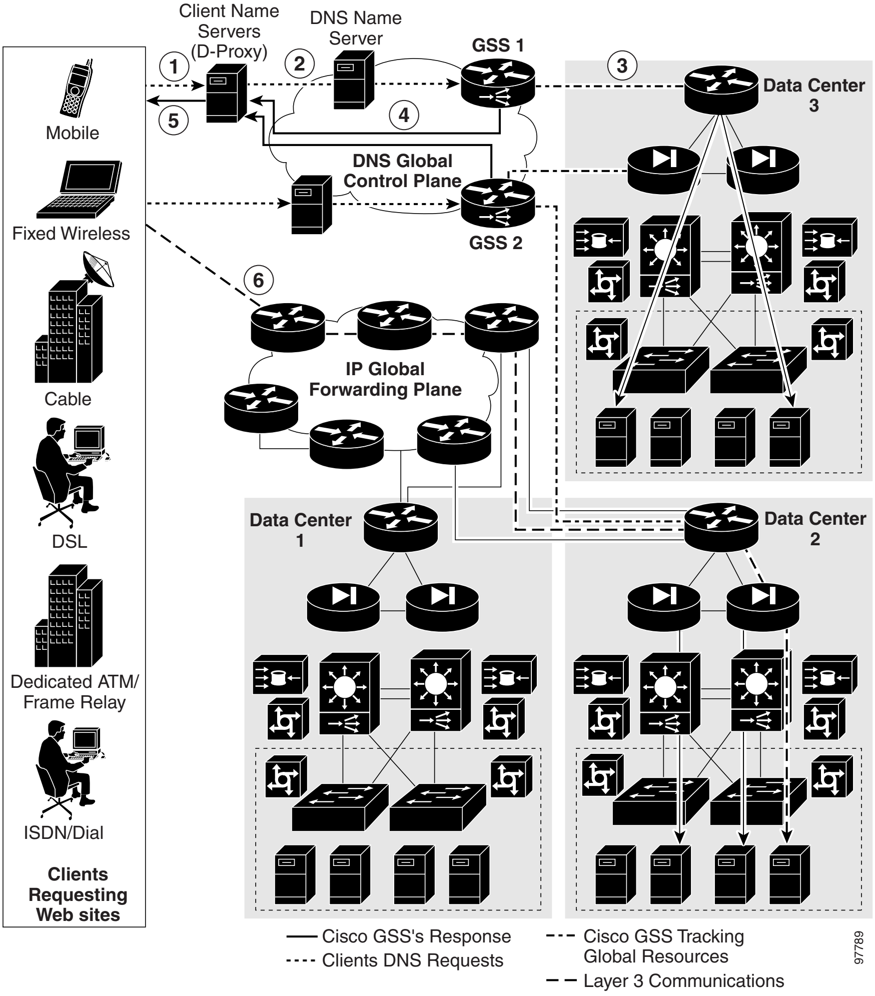
When resolving DNS requests, the GSS performs a series of distinct operations that take into account the resources under its control and return the best possible answer to the requesting client's D-proxy.

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



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 a the single, primary GSSM on a configured system.

GSS

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

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

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

Standby GSSM

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

When the standby GSSM operates as the interim primary GSSM, it contains a duplicate copy of the embedded GSS database currently installed on the primary GSSM. Both CLI and GUI support are also available on the standby GSSM once you configure it as the interim primary GSSM. While operating as the primary GSSM, you can monitor GSS behavior and make configuration changes, as necessary.

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

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

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

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

DNS Rules

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

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

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

Each DNS rule takes into account the following variables:

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

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

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

Each GSS network supports a maximum of 4000 DNS rules.

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

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

Locations and Regions

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

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

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

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

See Chapter 2, Configuring Resources, for information about configuring locations and regions.

Owners

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

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

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

See Chapter 2, Configuring Resources, for information about configuring owners.

Source Addresses and Source Address Lists

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

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

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

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

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 addresses:

```
192.168.1.110
192.168.1.110/32
192.168.1.0/24
192.168.0.0/16
```

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

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

See Chapter 4, Configuring Domain Lists, for information about configuring domain lists.

Answers and Answer Groups

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

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

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

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

As with domains and source addresses, answers are configured using the primary GSSM 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 CSS is routed to the best resource based on load and availability, as determined by the CSS. A request that is routed to a content routing agent (CRA) is routed to the best resource based on proximity, as determined in a DNS race conducted by the GSS.

See Chapter 6, Configuring Answers and Answer Groups, for information 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

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:

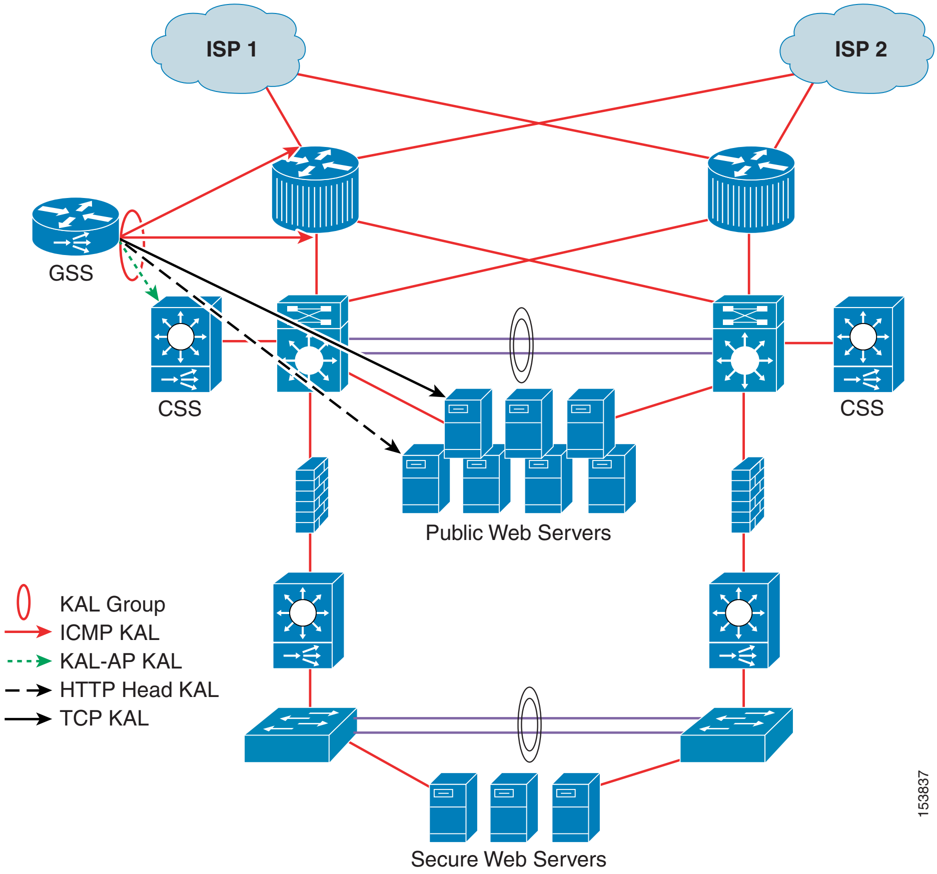
- ICMP
- TCP
- HTTP HEAD
- KAL-AP
- Scripted Keepalive
- Name Server
- None
- Adjusting Failure Detection Time for Keepalives

Multiport Keepalives

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

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

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



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

See Chapter 5, Configuring Keepalives, for information about modifying global keepalive parameters and creating shared keepalives.

ICMP

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

TCP

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

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

The GSS supports 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 IOS-compliant SLB, or Cisco LocalDirector. The HTTP HEAD keepalive type sends a TCP-formatted HTTP HEAD request to a web server at an address that you specify. The online status of the device is returned in the form of an HTTP Response Status Code of 200 (for example, HTTP/1.0 200 OK).

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

The GSS supports a maximum of 500 HTTP HEAD keepalives when using the standard detection method and a maximum of 100 HTTP HEAD keepalives when using the fast detection method. See the "Adjusting Failure Detection Time for Keepalives" section for details.

KAL-AP

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

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

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

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

Scripted Keepalive

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

Note A Scripted keepalive must always be a shared keepalive.

The GSS supports a maximum of 384 Scripted keepalives when using the standard detection method and 120 Scripted keepalives when using the fast detection method. See the "Adjusting Failure Detection Time for Keepalives" section for more details. Seconday 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.

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

(*# Ack'd Packets* * (*Response TO* + (*Retry TO* * *# of Retrie*s))) + *Timed Wait*

where:

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

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

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

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

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

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

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

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

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

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

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

(1 * (2 + (2 * 1))) + 0 = 4 seconds

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

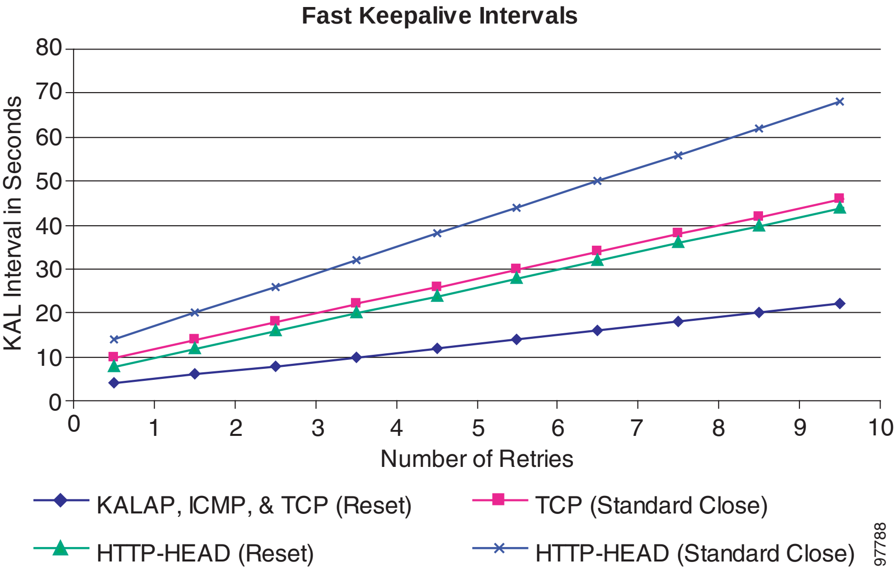
The GSS associates the number of retries value with every packet that requires some form of acknowledgement before continuing with a keepalive cycle (ICMP requests, TCP SYN, or TCP FIN). For example, to fully complete a TCP-based keepalive cycle, the TCP-based keepalive retries the SYN packet for the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

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

(1 * (2 + (2 * 5))) + 0 = 12 seconds

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

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



You can also define the number of consecutive successful keepalive attempts (probes) that must occur before the GSS identifies that an offline answer is online. The GSS monitors each keepalive attempt to determine if the attempt was successful. The 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

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.

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

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

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

See the "Balance Method Options for Answer Groups" section for information about how the GSS determines which answer to select when using the ordered list balance method.

Round-Robin Method

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

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

See the "Balance Method Options for Answer Groups" section for information about how the GSS determines which answer to select when using the round-robin balance method.

Weighted Round-Robin Method

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

See the "Balance Method Options for Answer Groups" section for information about how the GSS determines which answer to select when using the weighted round-robin balance method.

Least-Loaded Method

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

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

See the "Balance Method Options for Answer Groups" section for information 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

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

Table 1-2 Answer Group Options (continued)

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

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

- Order
- Weight
- Load Threshold

Order

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

Weight

Use the 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 *n* 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 undisrupted services and remain open for business by supporting persistent sticky network connections between customers and e-commerce servers. Persistent network connections ensure that active connections are not interrupted and shopping carts are not lost before purchase transactions are completed.

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

This section contains the following topics:

- DNS Sticky GSLB
- Network Proximity GSLB

DNS Sticky GSLB

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

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

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

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

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

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

Network Proximity GSLB

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

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

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

See Chapter 9, Configuring Network Proximity, for information about configuring proximity for GSS devices in your network.

DDoS Detection and Mitigation

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

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

In such cases, the following network points are affected:

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

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

Typically, the DDoS module prevents the following:

- Reflector attacks where the attacker spoofs the IP address of the victim (that is, the GSS). See the "Mitigation Rules" section for more information.

- Attacks where malformed DNS packets are transmitted
- Attacks where DNS queries are sent:
  - For any domain (that is, a DoS replay attack) from a specific source IP.
  - For domains not configured on the GSS
  - From different source IPs globally exceeding the GSS packet processing rate.
  - From spoofed IP addresses

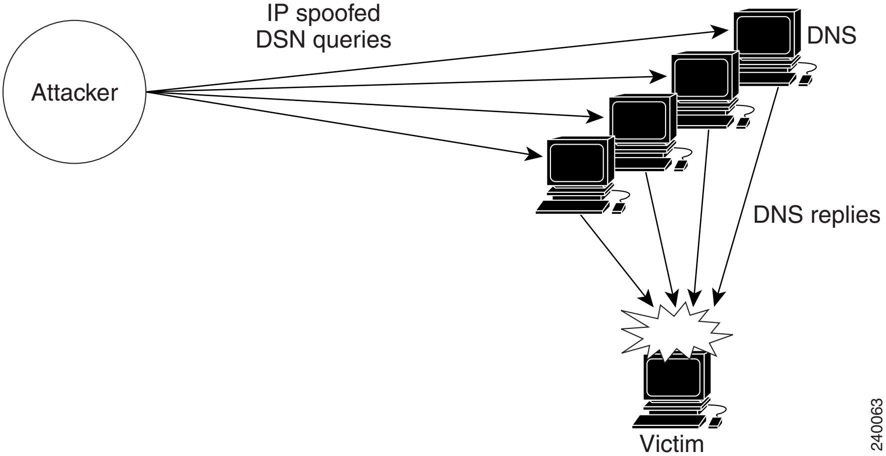
The DDoS module prevents these attacks by performing three primary functions, each of which is explained in the sections that follow:

- Mitigation Rules
- Rate-Limits
- Anti-Spoofing Mechanism

Mitigation Rules

A reflector attack occurs when the attacker spoofs the IP address of the victim (in this case, the GSS) and sends multiple DNS requests to a DNS server or multiple DNS servers posing as the victim (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



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

- Packets are dropped with a source port of 53 and QR bit of 1 (response) when responses come from a source port other than 53.
- Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.
- Queries are dropped with a payload length smaller than 12 bytes.
- Packets are dropped with a source port equal to 53, but less than 1024, and a QR bit of 0 (request).

By default, mitigation rules are enabled.

Rate-Limits

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

Note The final rate limits for each D-proxy and the global rate limit are determined by multiplying the rate-limits learned during peacetime (or configured via the CLI) with a tolerance factor.

Anti-Spoofing Mechanism

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

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

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

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

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

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

See Chapter 10, Displaying GSS Global Server Load-Balancing Statistics, for instructions on how to monitor DDoS statistics. See the *Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide* for specific procedures on how to enable DDoS prevention and configure filters, rate limits, and anti-spoofing.

GSS Network Deployment

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

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

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

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

- Locating GSS Devices
- Locating GSS Devices Behind Firewalls
- Communication Between GSS Nodes
- Deployment Within Data Centers

Locating GSS Devices

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

Because the GSS serves as the authoritative name server for one or more domains, each GSS must be publicly or privately addressable on your enterprise network to allow 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 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.

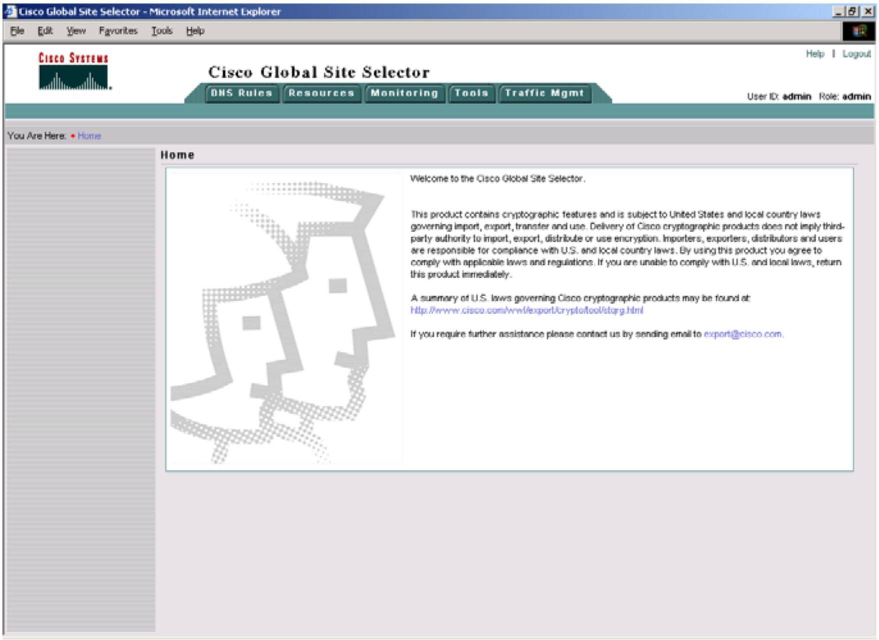
Understanding the Primary GSSM GUI

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 Netscape Navigator Version 4.79 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, you can 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 (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


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
You Are Here: • Home
Home
148645

User ID: admin Role: admin

Welcome to the Cisco Global Site Selector.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

The following sections describe the organization and structure of the primary GSSM GUI:

- 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 page. List pages and details pages are described in the sections that follow.

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.

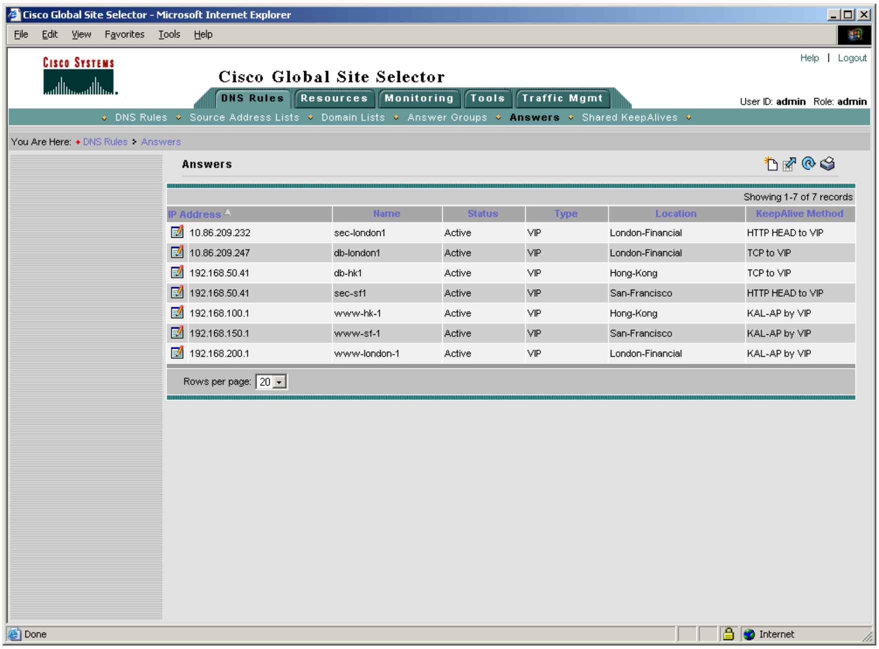
List pages display all data in tabular format to provide you with a detailed view of the resources available on your GSS network. In addition, you can use list pages to add new resources (for example, DNS rules or answer groups) or modify existing resources.

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 containing the information that you wish 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.

Figure 1-8 shows an example of a primary GSSM Answers list page.

Figure 1-8 Answers List Page



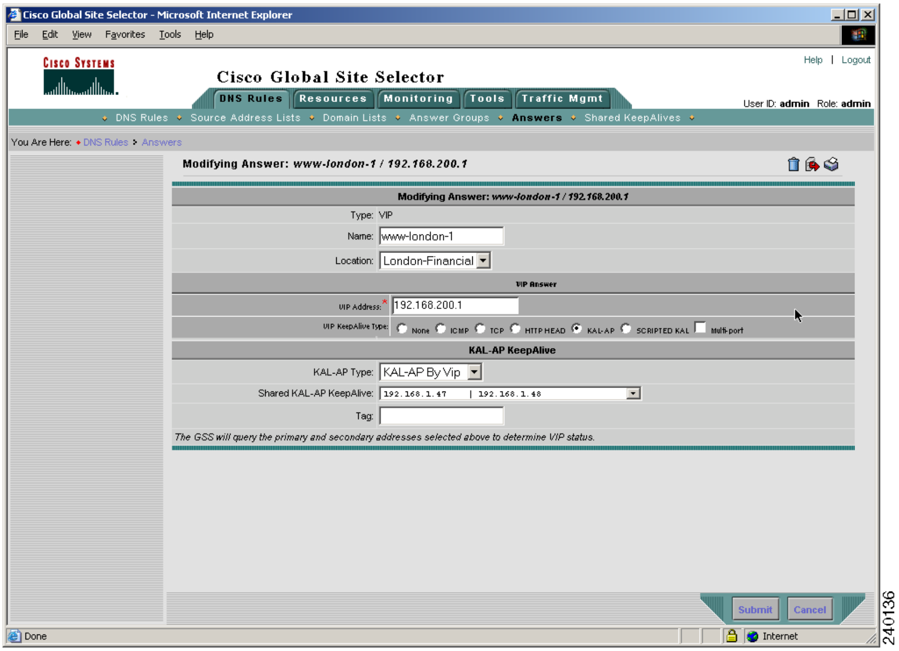
IP Address	Name	Status	Type	Location	KeepAlive Method
10.86.209.232	sec-london1	Active	VIP	London-Financial	HTTP HEAD to VIP
10.86.209.247	db-london1	Active	VIP	London-Financial	TCP to VIP
192.168.50.41	db-hk1	Active	VIP	Hong-Kong	TCP to VIP
192.168.50.41	sec-sf1	Active	VIP	San-Francisco	HTTP HEAD to VIP
192.168.100.1	www-hk-1	Active	VIP	Hong-Kong	KAL-AP by VIP
192.168.150.1	www-sf-1	Active	VIP	San-Francisco	KAL-AP by VIP
192.168.200.1	www-london-1	Active	VIP	London-Financial	KAL-AP by VIP

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 (see Figure 1-8). Next to each answer is an icon that show a pad and pencil, called the Modify icon. Click the Modify icon to display the details page for that answer (Figure 1-9). From the Modifying Answer details page, modify the properties of an answer or delete the answer.

Figure 1-9 Modifying Answer Details Page



Modifying Answer: *www-london-1 / 192.168.200.1*

Modifying Answer: *www-london-1 / 192.168.200.1*

Type: VIP

Name: www-london-1

Location: London-Financial

VIP Answer

VIP Address:* 192.168.200.1

VIP KeepAlive Type: ○ None ○ ICMP ○ TCP ○ HTTP HEAD ● KAL-AP ○ SCRIPTED KAL □ Multi-port

KAL-AP KeepAlive

KAL-AP Type: KAL-AP By Vip

Shared KAL-AP KeepAlive: 192.168.1.47 | 192.168.1.48

Tag:

The GSS will query the primary and secondary addresses selected above to determine VIP status.

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

Icon or Symbol	Purpose	Location
📝	Modify icon. Opens the associated item for editing in a details page, displaying configuration settings on the details page.	List pages
▼	Sort icon. Indicates that the items listed in a list table are sorted in descending order according to the property listed in this column.	List pages
📄	Create icon/Open DNS Rules Builder icon. Opens the associated details page to accept user input for configuration.	List pages
🖨	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.	List pages and Detail pages

Table 1-3 GSSM GUI Icons and Symbols (continued)

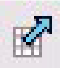
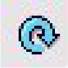
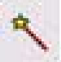
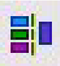
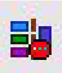
Icon or Symbol	Purpose	Location
	Export to CSV icon. When you view GSS resources or monitor GSS network activity, Export allows you to save data displayed in the window to a comma-delimited flat file for use in other applications.	List pages
	Refresh icon. When you view GSS resources or monitor GSS network activity, Refresh forces the GUI page to update its content.	List pages
	Run Wizard icon. Opens the associated DNS rule for editing using the DNS Rules Wizard.	DNS Rules list page
	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.	DNS Rules list page
	Show All DNS Rules icon. Removes all filters, displaying a complete list of DNS rules for your GSS.	DNS Rules list page
*	Asterisk. Required field. Indicates that a value is required in the adjacent field before the item can be successfully saved.	Details pages

Table 1-3 GSSM GUI Icons and Symbols (continued)

Icon or Symbol	Purpose	Location
Submit	Submit icon. Saves the configuration information. When editing specific GSS system or device configuration information, Submit returns you to the associated list screen.	Detail pages
Cancel	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.	Detail pages
🗑	Delete icon. When you view configuration information for GSS resources, Delete allows you to delete the resource from the GSS network. **Note** 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.	Detail pages
Next >	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.	DNS Rules wizard

Table 1-3 GSSM GUI Icons and Symbols (continued)

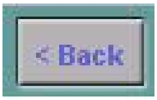
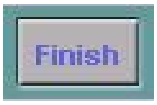
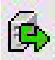
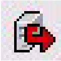
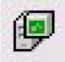
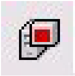
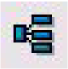
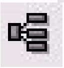
Icon or Symbol	Purpose	Location
	Back icon. Moves back to the previous page in the DNS Rules Wizard. You can also use the links under the Wizard Contents table of contents to move between steps in the wizard.	DNS Rules wizard
	Finish icon. Saves changes to the DNS rule. You return to the DNS Rules list page.	DNS Rules wizard
	Click to Add KAL icon. Adds multiple keepalives and/or destination ports to a single VIP-type answer.	Creating Answer and Modifying Answer details page
	Activate Answer icon. Reactivates a single suspended answer, all suspended answers in an answer group, all suspended answers associated with an owner, or all suspended answers associated with a location.	Modifying Answer, Modifying Answer Group, Modifying Owner, and Modifying Location detail page
	Suspend Answer icon. Temporarily stops the GSS from using a single answer, all answers in an answer group, all answers in all groups for an owner, or all answers in a location.	Modifying Answer, Modifying Answer Group, Modifying Owner, and Modifying Location detail page
	Activate DNS Rule icon. Reactivates a single suspended DNS Rule or all suspended DNS Rules associated with an Owner.	Modify DNS Rules and Modifying Owner detail pages

Table 1-3 GSSM GUI Icons and Symbols (continued)

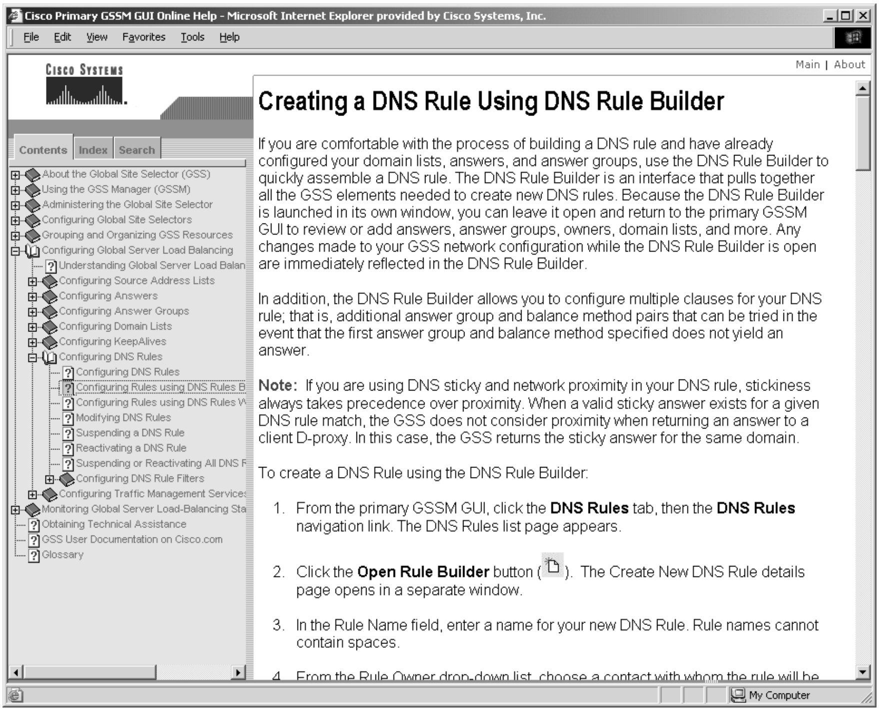
Icon or Symbol	Purpose	Location
	Suspend DNS Rules icon. Temporarily stops requests from being processed by a single DNS rule or all suspended DNS rules associated with an owner on your GSS.	Modify DNS Rules and Modifying Owner detail pages
	Set Answers KAL ICMP icon. Disassociates all answers from a selected shared keepalive and sets the keepalive type of each of those answers to ICMP using the answer's associated VIP.	Modifying Shared Keepalive details page
	Set Answers KAL None icon. Disassociates all answers from a selected shared keepalive and sets the keepalive type for each answer to none. The GSS assumes that the answers are always alive.	Modifying Shared Keepalive details page

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 (Figure 1-10), 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).

Figure 1-10 Primary GSSM GUI Online Help


Cisco Primary GSSM GUI Online Help - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Main | About
Contents Index Search
About the Global Site Selector (GSS)
Using the GSS Manager (GSSM)
Administering the Global Site Selector
Configuring Global Site Selectors
Grouping and Organizing GSS Resources
Configuring Global Server Load Balancing
Understanding Global Server Load Balan
Configuring Source Address Lists
Configuring Answers
Configuring Answer Groups
Configuring Domain Lists
Configuring KeepAlives
Configuring DNS Rules
Configuring DNS Rules
Configuring Rules using DNS Rules B
Configuring Rules using DNS Rules W
Modifying DNS Rules
Suspending a DNS Rule
Reactivating a DNS Rule
Suspending or Reactivating All DNS R
Configuring DNS Rule Filters
Configuring Traffic Management Services
Monitoring Global Server Load-Balancing Sta
Obtaining Technical Assistance
GSS User Documentation on Cisco.com
Glossary
My Computer
148644

Creating a DNS Rule Using DNS Rule Builder

If you are comfortable with the process of building a DNS rule and have already configured your domain lists, answers, and answer groups, use the DNS Rule Builder to quickly assemble a DNS rule. The DNS Rule Builder is an interface that pulls together all the GSS elements needed to create new DNS rules. Because the DNS Rule Builder is launched in its own window, you can 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.

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

Note: If you are using 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. In this case, the GSS returns the sticky answer for the same domain.

To create a DNS Rule using the DNS Rule Builder:

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

2. Click the **Open Rule Builder** button ( ). The Create New DNS Rule details 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

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.

Use the following order when configuring your GSS devices and resources from the primary GSSM for global server load balancing:

1. Create regions, locations, and owners—Optional. Use these groupings to organize your GSS network resources by customer account, physical location, owner, or other organizing principle. See Chapter 2, Configuring Resources for details.
2. Create one or more source address lists—Optional. Use these lists of IP addresses to identify the name servers (D-proxy) that forward requests for the specified domains. The default source address list is Anywhere to match any incoming DNS request to the domains. See Chapter 3, Configuring Source Address Lists for details.
3. Create one or more domain lists—Establish lists of Internet domains, possibly using wildcards, that are managed by the GSS and queried by users. See Chapter 4, Configuring Domain Lists for details.
4. Modify the default global keepalive settings or create any shared keepalives—Optional. These 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 8, Configuring DNS Sticky for details.
8. If you plan to use network proximity for your global server load balancing, configure proximity for GSS devices in your network—Proximity determines the best (most proximate) resource for handling global load-balancing requests. See Chapter 9, Configuring Network Proximity for details.

Where to Go Next

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

CHAPTER 2

Configuring Resources

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

This chapter contains the following major sections:

- Organizing Your GSS Network
- Creating and Modifying Locations and Regions
- Creating and Modifying Owners
- Grouping GSS Resources by Location, Region, and Owner
- Where to Go Next

Organizing Your GSS Network

The primary GSSM provides you the following tools 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

Keep in mind that it is not a requirement that regions and locations 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. We recommend that you create regions before you create locations because you associate a region with a location when creating the location.

This section includes the following procedures:

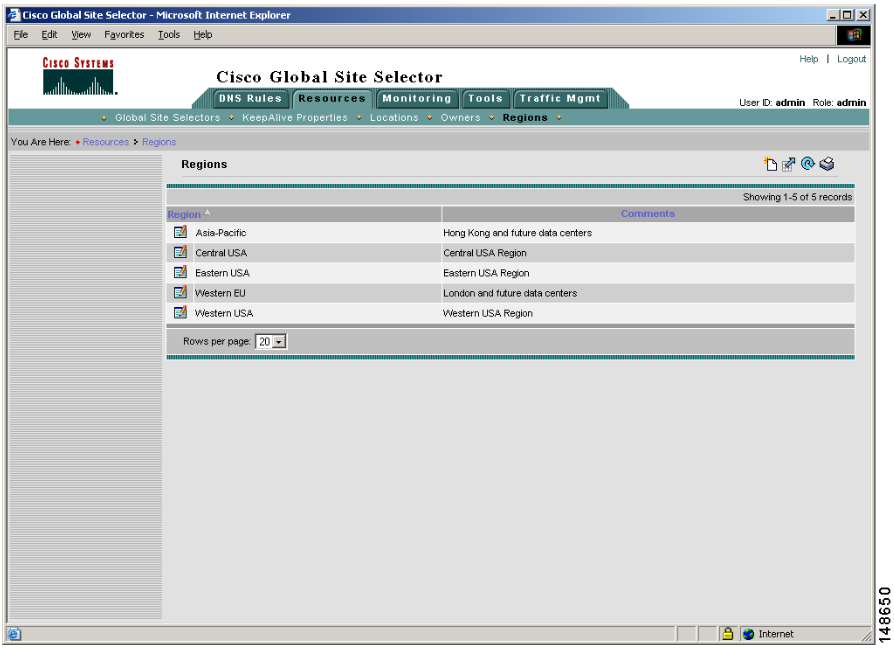
- Creating Regions
- Modifying Regions
- Creating Locations
- Modifying Locations
- Deleting Locations and Regions

Creating Regions

To create a region:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Regions** navigation link. The Regions list page appears (Figure 2-1).

Figure 2-1 Regions List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Regions
Internet
148650

Regions

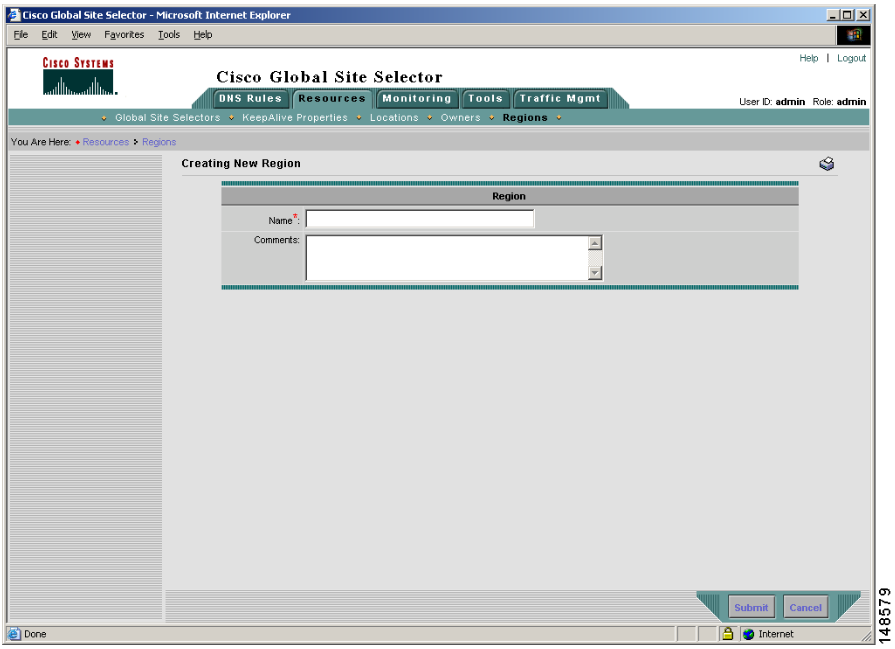
Showing 1-5 of 5 records

Region	Comments
Asia-Pacific	Hong Kong and future data centers
Central USA	Central USA Region
Eastern USA	Eastern USA Region
Western EU	London and future data centers
Western USA	Western USA Region

Rows per page: 20

3. Click the **Create Regions** icon. The Creating New Region details page appears (Figure 2-2).

Figure 2-2 Creating New Region Details Page



Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Regions
Done
Internet
Submit
Cancel
148579

Creating New Region

Region

Name*:

Comments:

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.

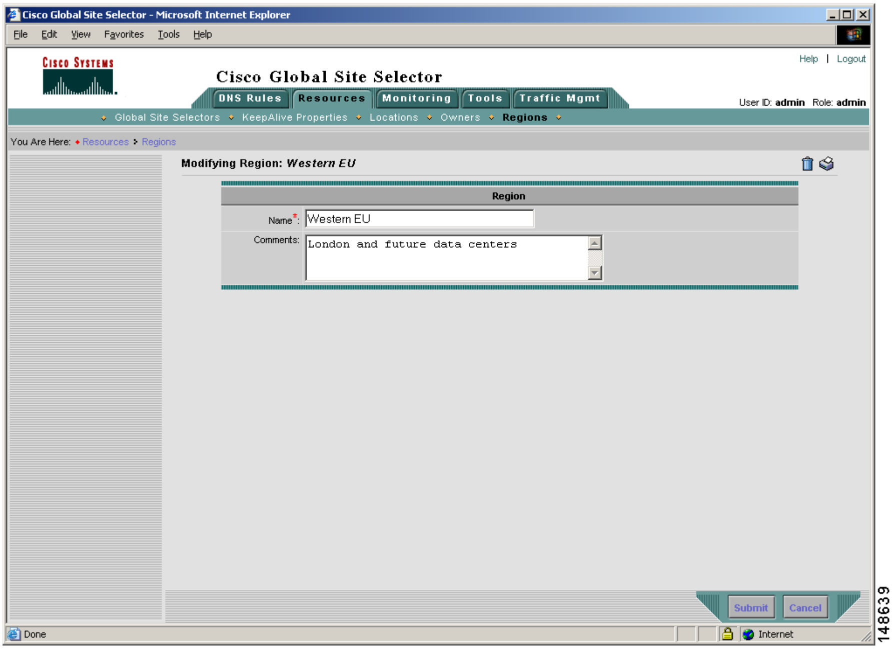
6. Click **Submit** to save changes to your new region and return to the Region list page. Your new region appears in the list and can be used to help you organize other GSS resources.

Modifying Regions

To modify a GSS region:

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 (Figure 2-3).

Figure 2-3 Modifying Region Details Page



Modifying Region: *Western EU*

Region

Name*: Western EU

Comments: London and future data centers

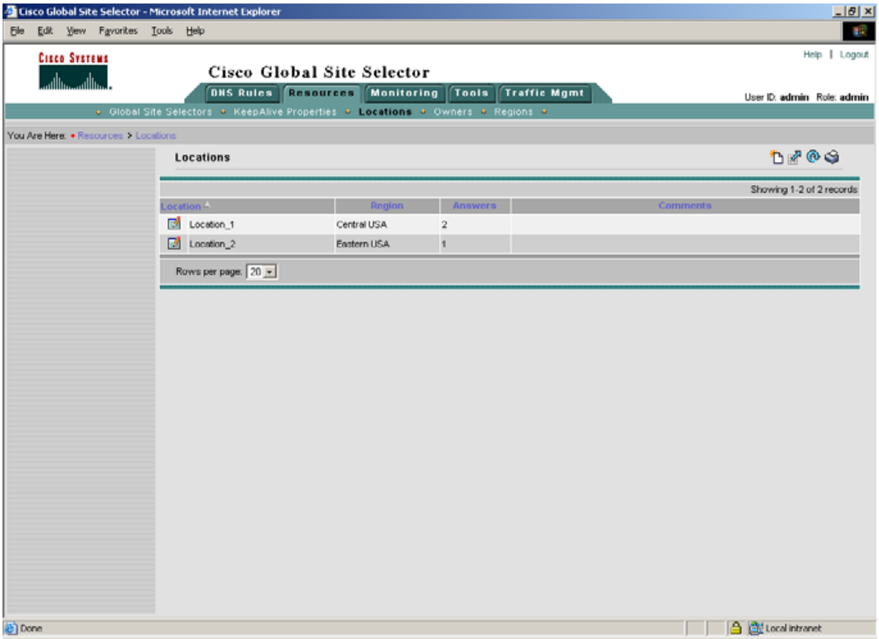
4. In the Name field, change the name of the region, if desired.
5. In the Comments field, enter or modify the descriptive information or notes regarding the region.
6. Click **Submit** to save the changes to your region and return to the Regions list page.

Creating Locations

To create a location:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Locations** navigation link. The Locations list page appears (Figure 2-4).

Figure 2-4 Locations List Page



User ID: admin Role: admin

You Are Here: • Resources > Locations

Locations

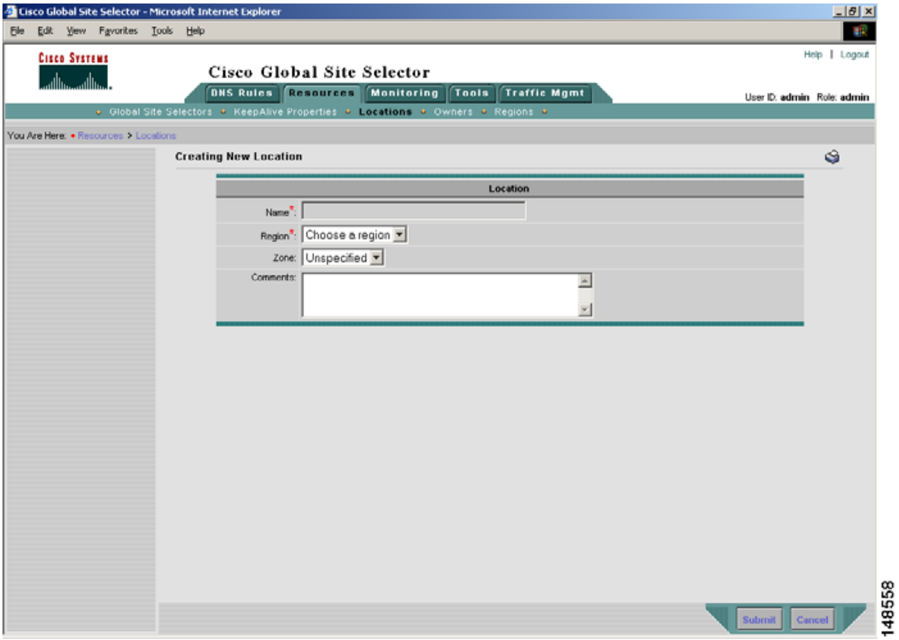
Showing 1-2 of 2 records

Location	Region	Answers	Comments
Location_1	Central USA	2	
Location_2	Eastern USA	1	

Rows per page: 20

3. Click the **Create Location** icon. The Creating New Location details page appears (Figure 2-5).

Figure 2-5 Creating New Location Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Locations
Submit
Cancel
148558

Creating New Location

Location

Name*:

Region*: Choose a region

Zone: Unspecified

Comments:

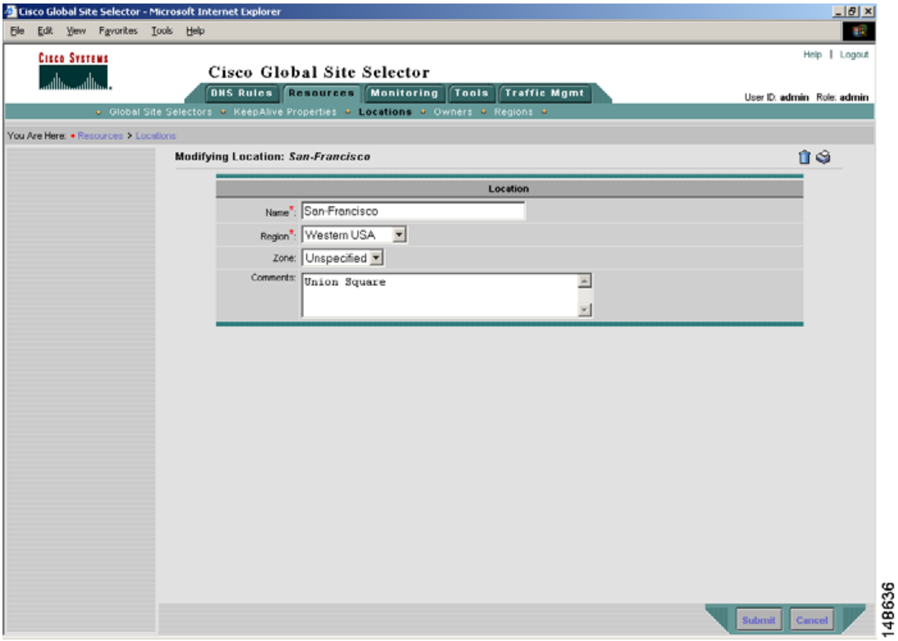
4. In the Name field, enter the name for your new location.
5. Click the **Region** drop-down list and choose a region with which the location will be associated. There should be a logical connection between the region and location.
6. If performing network proximity, click the **Zone** drop-down list 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:

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 (Figure 2-6).

Figure 2-6 Modifying Location Details Page



Modifying Location: *San-Francisco*

Location

Name*: San-Francisco
Region*: Western USA
Zone: Unspecified
Comments: Union Square

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. Refer to the *Global Site Selector Administration Guide* for details.

To delete regions and locations:

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

If an error appears informing you that a GSS resource is still linked to the region or location you want to delete, disassociate that resource and then attempt to delete the grouping again.

Creating and Modifying Owners

Owners are logical groupings for GSS network resources that correspond to business or organizational structures. For example, an owner might be a hosting customer, an internal department such as human resources, or an IT staff resource.

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

For information on using owners to manage your GSS network, see the following chapters and sections:

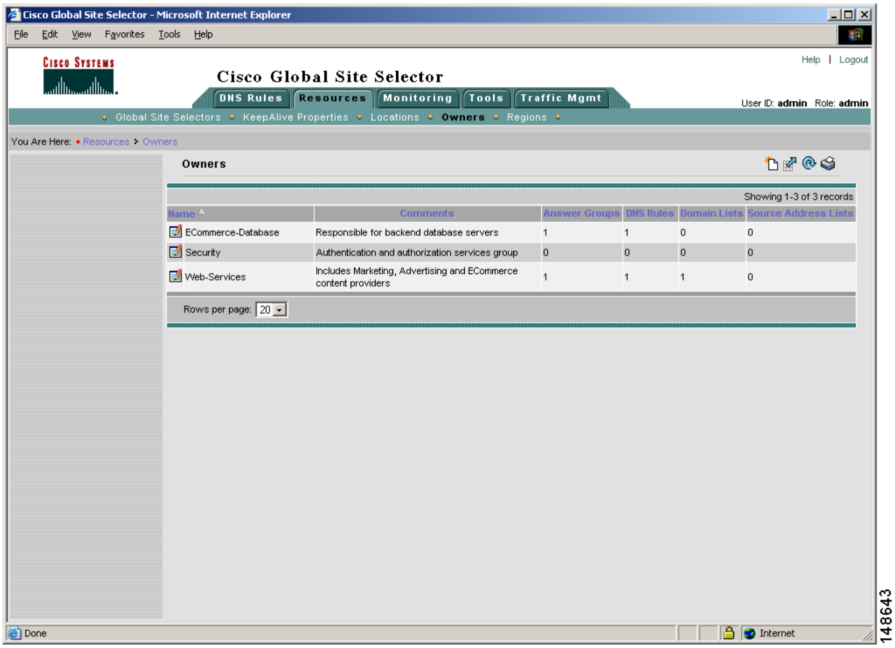
- Refer to the Suspending or Reactivating All Answers in an Answer Group Associated with an Owner section in Chapter 6, Configuring Answers and Answer Groups
- Refer to the Suspending or Reactivating All DNS Rules Belonging to an Owner section in Chapter 7, Building and Modifying DNS Rules

Creating Owners

To create an owner:

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 (Figure 2-7).

Figure 2-7 Owners List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Owners
Owners
Done
Internet
148643

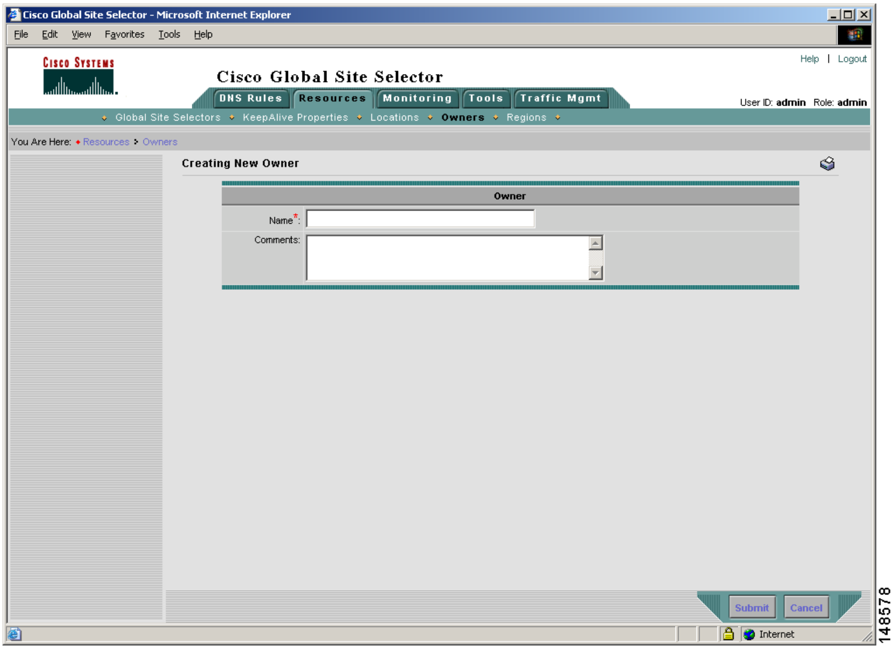
Showing 1-3 of 3 records

Name	Comments	Answer Groups	DNS Rules	Domain Lists	Source Address Lists
ECommerce-Database	Responsible for backend database servers	1	1	0	0
Security	Authentication and authorization services group	0	0	0	0
Web-Services	Includes Marketing, Advertising and ECommerce content providers	1	1	1	0

Rows per page: 20

3. Click the **Create Owner** icon. The Creating New Owner details page appears (Figure 2-8).

Figure 2-8 Creating New Owner Details Page



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.

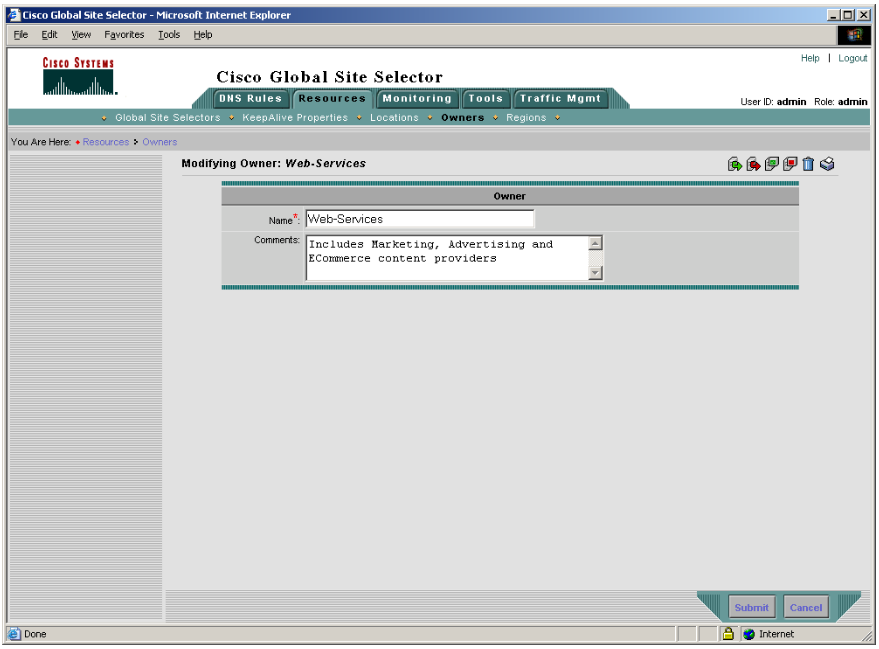
6. Click **Submit** to save the new owner and return to the Owners list page. Your new owner is listed and can now be used to help you organize other GSS resources.

Modifying Owners

To modify an owner:

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 (Figure 2-9).

Figure 2-9 Modifying Owner Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Help | Logout
Cisco Systems
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Owners
Submit
Cancel
Done
Internet
148637

Modifying Owner: *Web-Services*

Owner

Name*: Web-Services

Comments: Includes Marketing, Advertising and ECommerce content providers

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. Refer to the *Global Site Selector Administration Guide* for details.

To delete an owner:

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 2-1 GSS Network Groupings

GSS Network Resource	Grouped By	Grouped Using
GSS	Location	Global Site Selector details page
Locations	Region	Locations details page
Region	—	—
Owner	—	—
DNS rules	Owner	DNS Rule Builder DNS Rule Wizard
Source address lists	Owner	Source Address Lists details page
Domain lists	Owner	Domain Lists details page
Answer group	Owner	Answer Group details page
Answer	Location	Answer details page

Where to Go Next

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

CHAPTER 3

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 through the creation of source address lists, 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, up to 30 addresses for each list, to represent the DNS proxies from which requests originate. Each GSS supports up to 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:

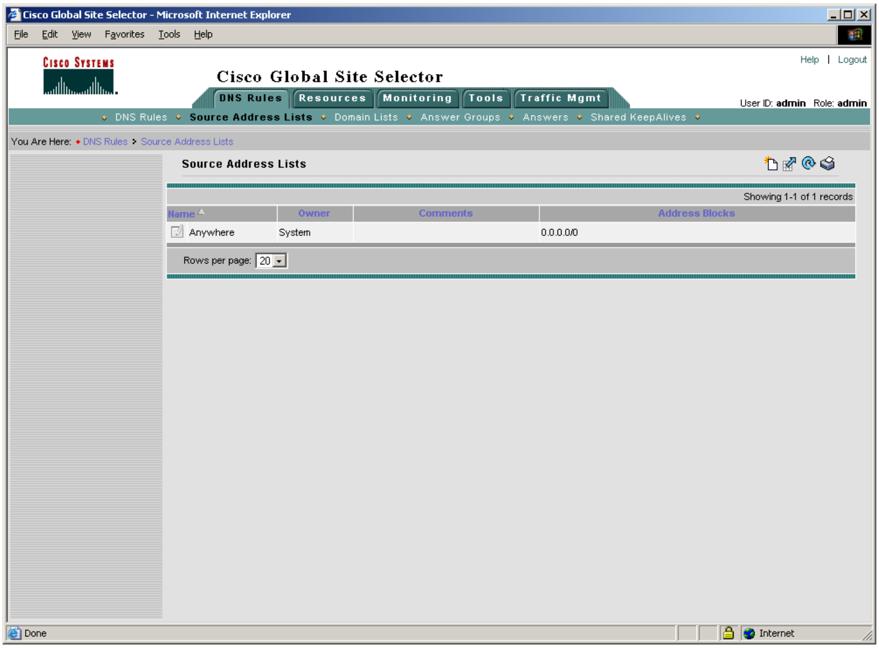
- Creating Source Address Lists
- Modifying Source Address Lists
- Deleting Source Address Lists
- Where to Go Next

Creating Source Address Lists

To configure a source address list:

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 (Figure 3-1).

Figure 3-1 Source Address Lists List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules Source Address Lists
Rows per page: 20
Done
Internet
148658

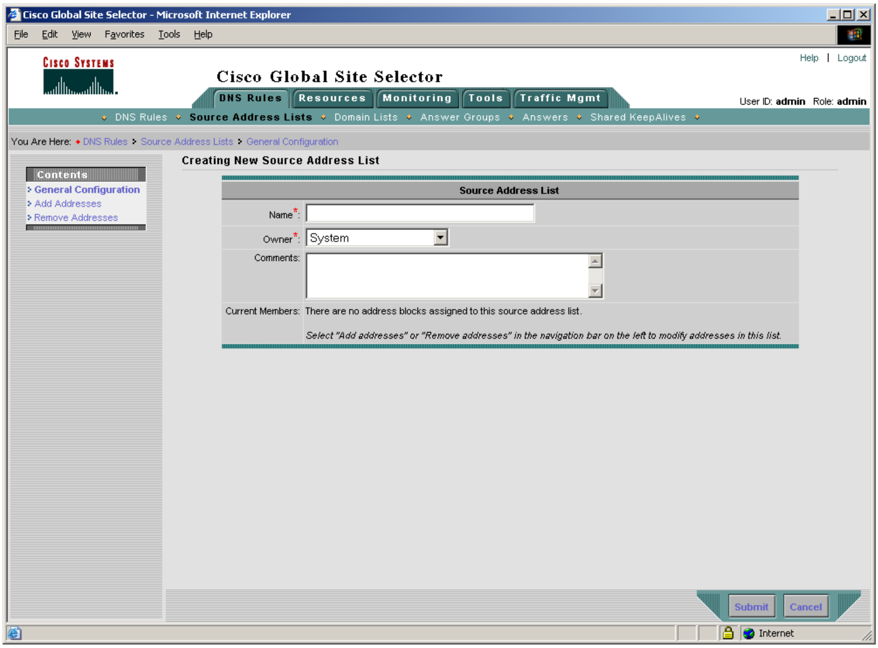
Source Address Lists

Showing 1-1 of 1 records

Name	Owner	Comments	Address Blocks
Anywhere	System		0.0.0.0/0

3. Click the **Create Source Address List** icon. The Creating New Source Address List details page appears (Figure 3-2).

Figure 3-2 Creating New Source Address List—General Configuration



Creating New Source Address List

Source Address List

Name*:

Owner*: System

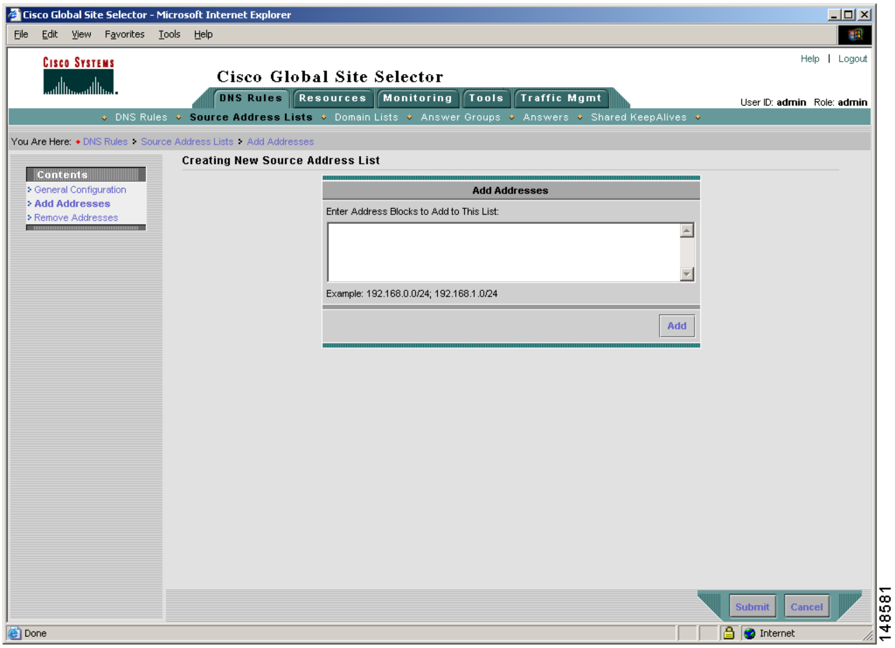
Comments:

Current Members: There are no address blocks assigned to this source address list.

Select "Add addresses" or "Remove addresses" in the navigation bar on the left to modify addresses in this list.

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 (Figure 3-3).

Figure 3-3 Creating New Source Address List—Add Addresses


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Source Address Lists > Add Addresses
Contents
General Configuration
Add Addresses
Remove Addresses
Creating New Source Address List
Add Addresses
Enter Address Blocks to Add to This List:
Example: 192.168.0.0/24; 192.168.1.0/24
Add
Submit
Cancel
Done
Internet
148581

6. In the Add Addresses section of the page, perform the following:

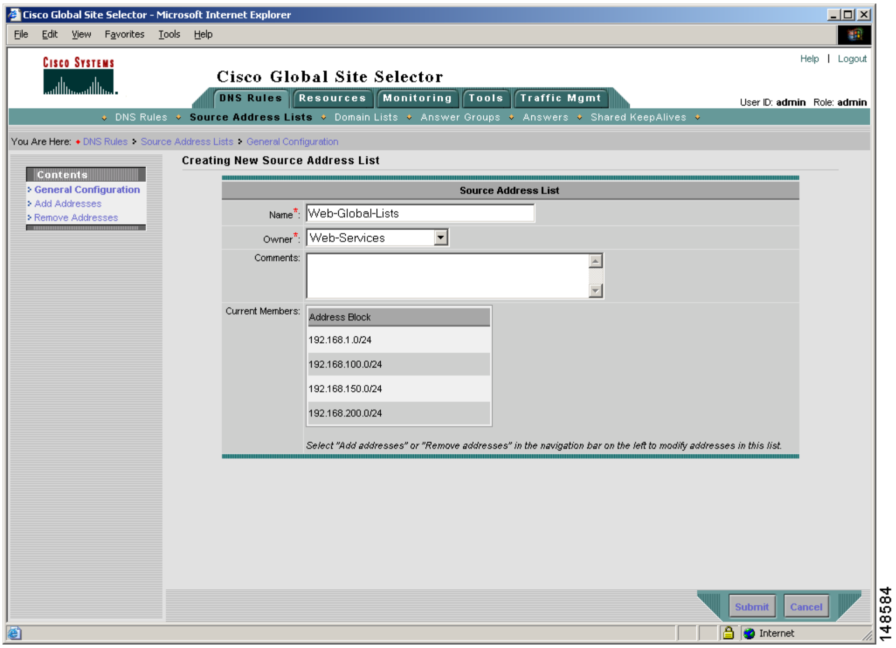
   a. Enter the IP addresses or CIDR address blocks of the client DNS proxies. You use this interface to add new addresses or address blocks to your list of source addresses. If entering multiple addresses, separate each address with a semicolon. You can enter up to 30 addresses for each list. For example, enter the following:

   ```
   192.168.100.0/24; 172.16.0.0/16; 172.16.10.1
   ```

   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 (Figure 3-4).

Figure 3-4 Creating Source Address List—Current Members List



Creating New Source Address List

Source Address List

Name*: Web-Global-Lists

Owner*: Web-Services

Comments:

Current Members:

Address Block
192.168.1.0/24
192.168.100.0/24
192.168.150.0/24
192.168.200.0/24

Select "Add addresses" or "Remove addresses" in the navigation bar on the left to modify addresses in this list.

8. When you are satisfied with your Source Address List, click the **Submit** button to save your changes and return to the Source Address Lists list page.

Modifying Source Address Lists

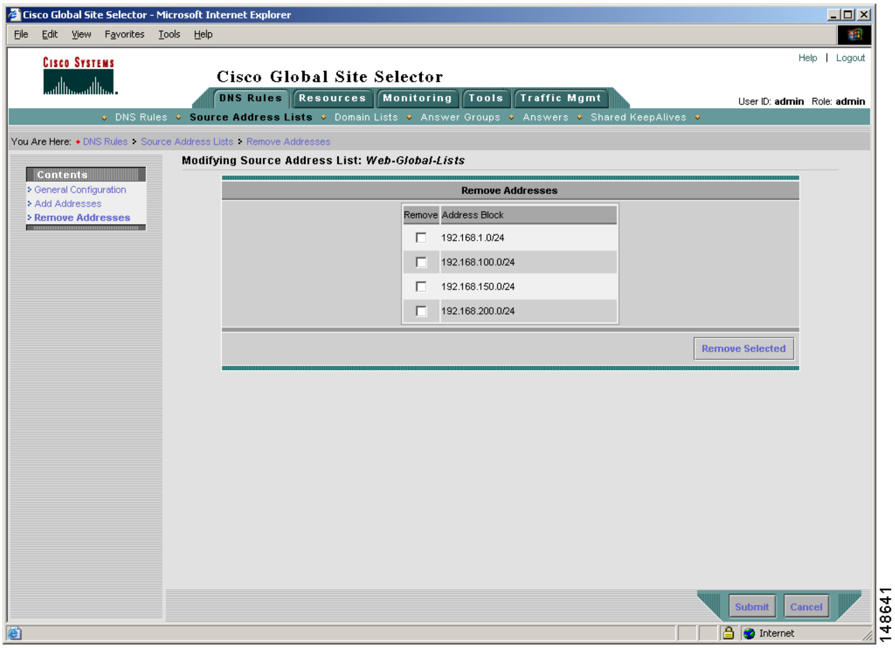
To modify an existing source address list:

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 (see Figure 3-2). Source address list names cannot contain spaces.

4. To add more source addresses to the list, click the **Add Addresses** navigation link. Use the field provided (see Figure 3-3) 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. To remove addresses from the Source Address List, click the **Remove Addresses** navigation link. The Remove Addresses section of the page appears (Figure 3-5). Click the check box accompanying each source address that you want to remove from the list, then click the **Remove Selected** button to remove the selected source addresses from the list.

Figure 3-5 Modifying Source Address List—Remove Addresses


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > Source Address Lists > Remove Addresses
Contents
General Configuration
Add Addresses
Remove Addresses
Remove Selected
Submit
Cancel
Internet
148641

Modifying Source Address List: *Web-Global-Lists*

Remove Addresses

Remove	Address Block
□	192.168.1.0/24
□	192.168.100.0/24
□	192.168.150.0/24
□	192.168.200.0/24

6. Review your updated source address list under the Current Members section of the details page (see Figure 3-4).

7. 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. Refer to Chapter 7, Building and Modifying DNS Rules, for information about modifying a DNS rule.

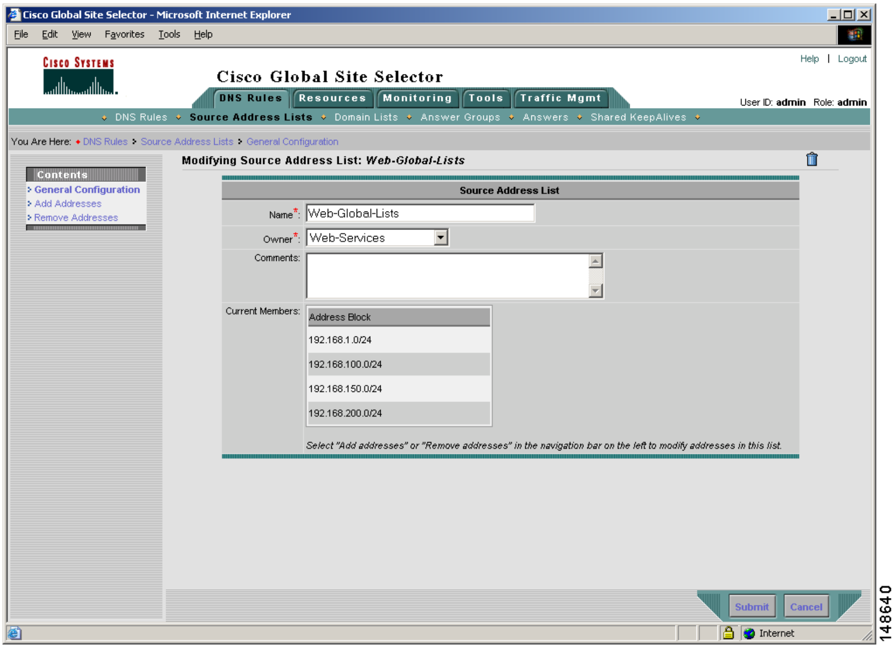
Caution Deletions of any kind cannot be undone in the primary GSSM. Before deleting any data that you think you might want to use at a later point in time, perform a database backup of your GSSM. Refer to the *Global Site Selector Administration Guide* for details.

To delete a source address list from your GSS network:

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 (Figure 3-6). The GSS software prompts you to confirm your decision to delete the Source Address List.

   Note If an error appears informing you that the source address list is referenced by an existing DNS rule, deselect the source address list from the DNS rule, then attempt to delete the source address list again. Refer to Chapter 7, Building and Modifying DNS Rules, for information about modifying a DNS rule.

Figure 3-6 Modifying Source Address List—Delete Icon


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > Source Address Lists > General Configuration
Contents
General Configuration
Add Addresses
Remove Addresses
Submit
Cancel
Internet
148640

Modifying Source Address List: *Web-Global-Lists*

Source Address List

Name*: Web-Global-Lists

Owner*: Web-Services

Comments:

Current Members:

Address Block
192.168.1.0/24
192.168.100.0/24
192.168.150.0/24
192.168.200.0/24

Select "Add addresses" or "Remove addresses" in the navigation bar on the left to modify addresses in this list.

5. Click **OK** to confirm your decision. You return to the Source Address Lists list page. The source address list is removed from the 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.

CHAPTER 4

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:

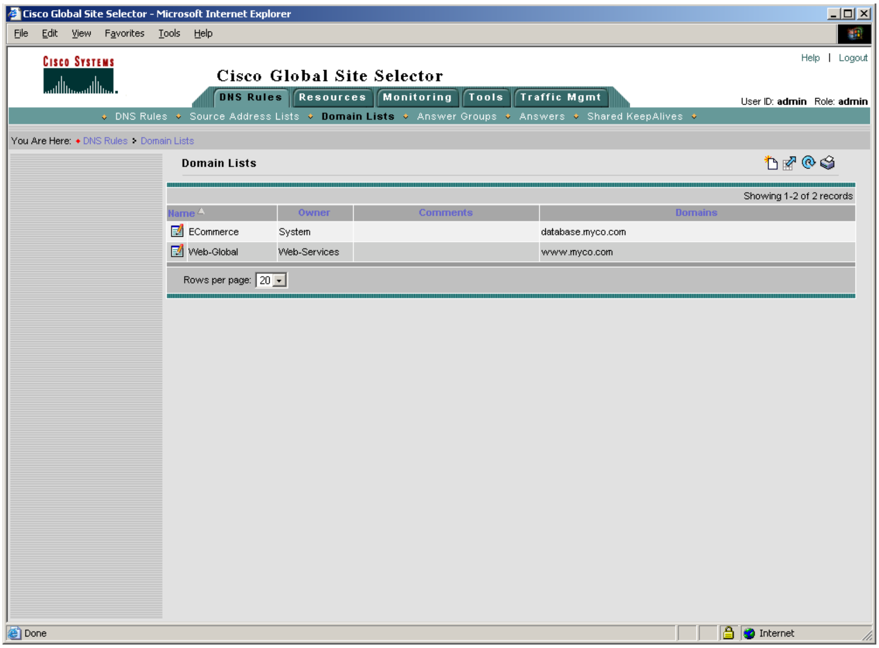
- Creating Domain Lists
- Modifying Domain Lists
- Deleting Domain Lists
- Where to Go Next

Creating Domain Lists

To create a domain list:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Domain Lists** navigation link. The Domain Lists list page appears (Figure 4-1).

Figure 4-1 Domain Lists Page



User ID: admin Role: admin

You Are Here: DNS Rules > Domain Lists

Domain Lists

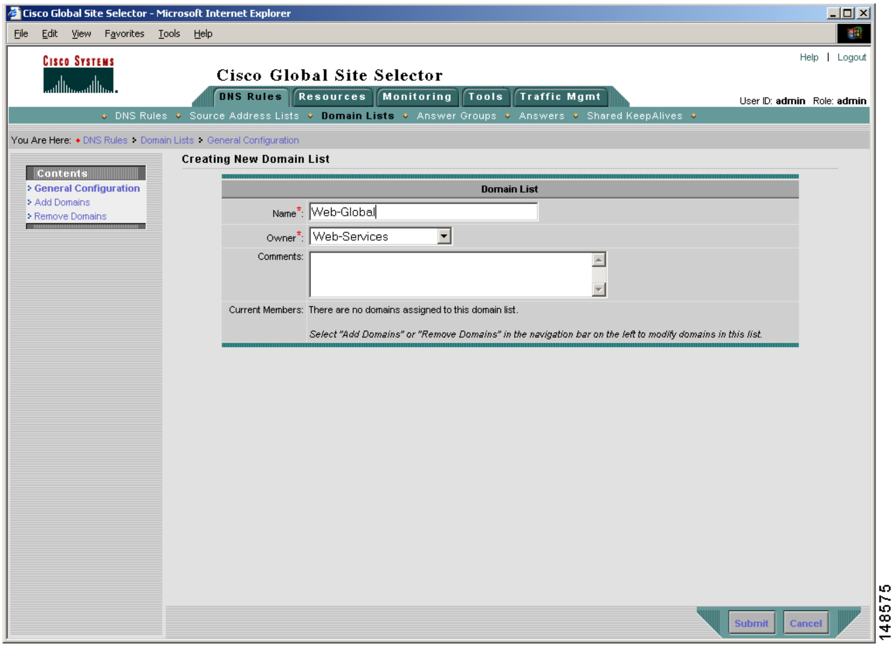
Showing 1-2 of 2 records

Name	Owner	Comments	Domains
ECommerce	System		database.myco.com
Web-Global	Web-Services		www.myco.com

Rows per page: 20

3. Click the **Create Domain List** icon. The Creating New Domain List details page appears. (Figure 4-2.)

Figure 4-2 Creating New Domain List Details Page—General Configuration



Name*: Web-Global

Owner*: Web-Services

Comments:

Current Members: There are no domains assigned to this domain list.

Select "Add Domains" or "Remove Domains" in the navigation bar on the left to modify domains in this list.

4. In the General Configuration details page (**General Configuration** navigation link), perform the following:

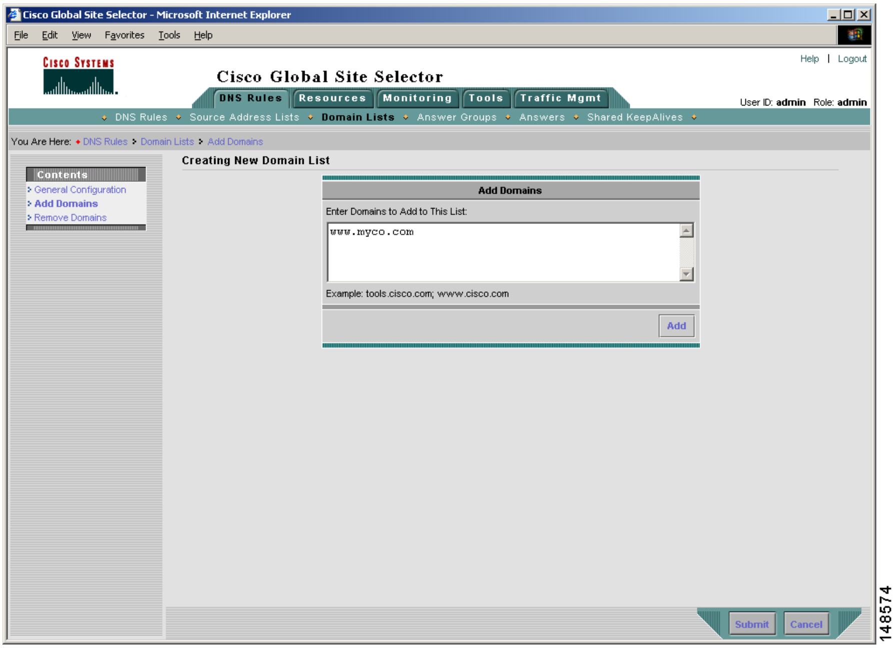
   a. In the Name field, enter a name for the new domain list. Domain list names cannot contain spaces.

   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.

Figure 4-3 Creating New Domain List—Add Domains



Creating New Domain List

Add Domains

Enter Domains to Add to This List:

```
www.myco.com
```

Example: tools.cisco.com; www.cisco.com

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.

   Note the following 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.

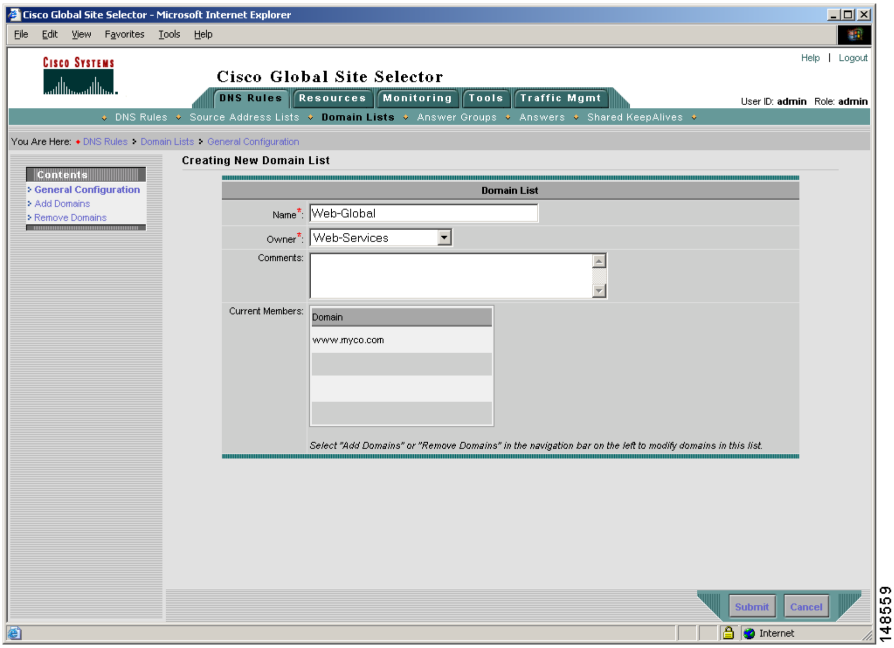
  For example, assume that you have 20 or more possible domains that the GSS is responsible, such as www1.cisco.com, www2.cisco.com, and so on. You can create a wildcard expression that covers all of those domains:

  ```
  .*\.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 (Figure 4-4).
9. Click the **Submit** button to save your domain list changes and return to the Domain List lists page.

Figure 4-4 Creating Domain List—Current Members List



Creating New Domain List

Domain List

Name*: Web-Global

Owner*: Web-Services

Comments:

Current Members:

Domain
www.myco.com

Select "Add Domains" or "Remove Domains" in the navigation bar on the left to modify domains in this list.

Modifying Domain Lists

To modify an existing domain list:

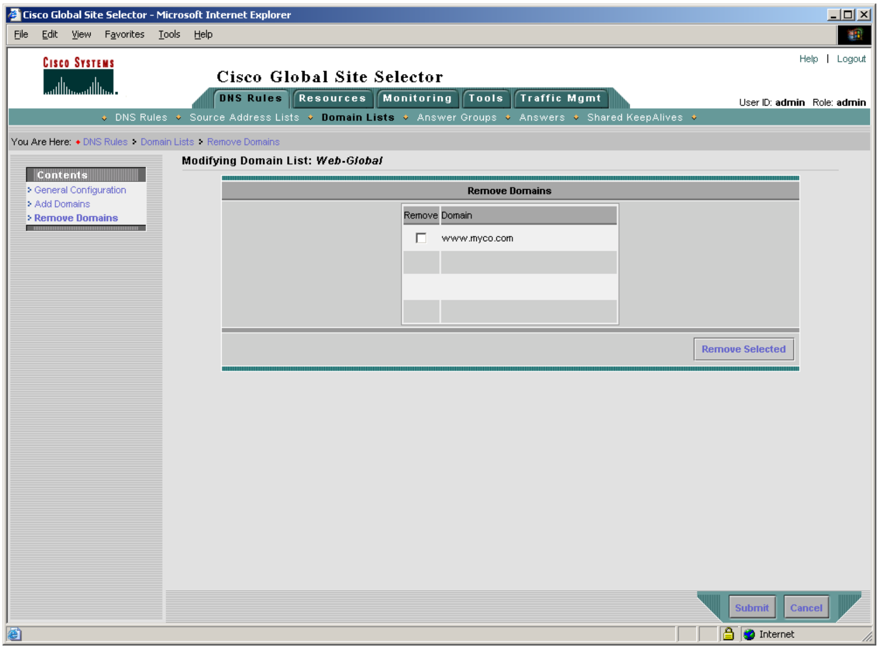
1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Domain Lists** navigation link. The Domain Lists list page appears (see Figure 4-1).
3. From the Domain Lists list, click the **Modify Domain List** icon located to the left of the domain list that you want to modify. The Modifying 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 (see Figure 4-2). Domain list names cannot contain spaces.

5. To add more domains to the list, click the **Add Domains** navigation link. Use the text box (see Figure 4-3) 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 (Figure 4-5). Click the check box accompanying each domain that you want to remove from the list, then click the **Remove Selected** button. The GSS removes the deleted domain lists from the page.

Figure 4-5 Modifying Domain List—Remove Domains



User ID: admin Role: admin

You Are Here: DNS Rules > Domain Lists > Remove Domains

Modifying Domain List: *Web-Global*

Remove Domains

Remove	Domain
□	www.myco.com

148633

7. Review your updated domain lists under the Current Members section of the details page (see Figure 4-4).

8. Click the **Submit** button to save your changes and return to the Domain List list page.

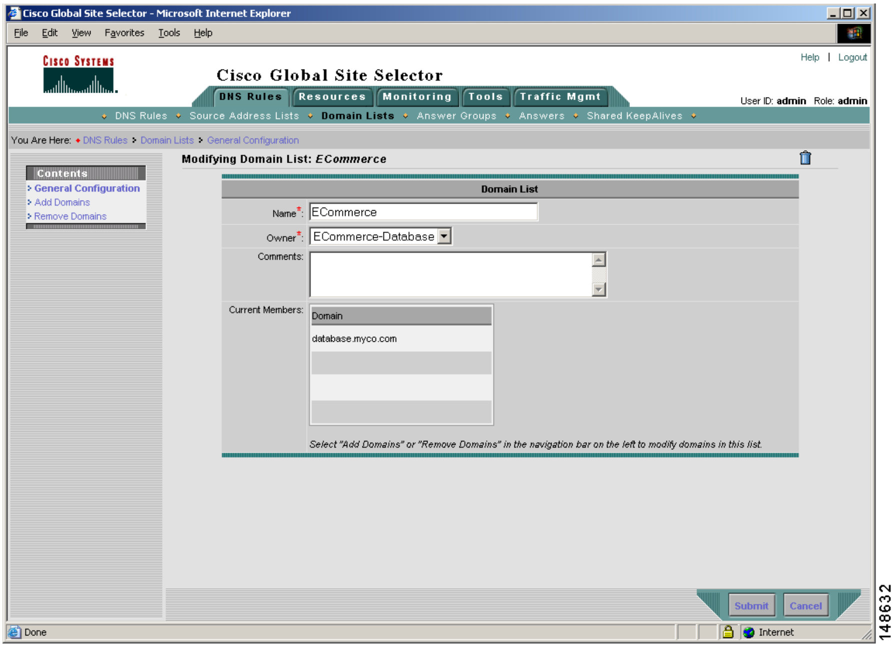
Deleting Domain Lists

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. Refer to Chapter 7, Building and Modifying DNS Rules, for information about modifying a DNS rule.

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

To delete a domain list 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 (Figure 4-6).



Modifying Domain List: *ECommerce*

Domain List

Name*: ECommerce

Owner*: ECommerce-Database

Comments:

Current Members:

Domain
database.myco.com

Select "Add Domains" or "Remove Domains" in the navigation bar on the left to modify domains in this list.

Figure 4-6 Modifying Domain List—Delete Icon

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. Refer to Chapter 7, Building and Modifying DNS Rules.

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.

CHAPTER 5

Configuring Keepalives

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

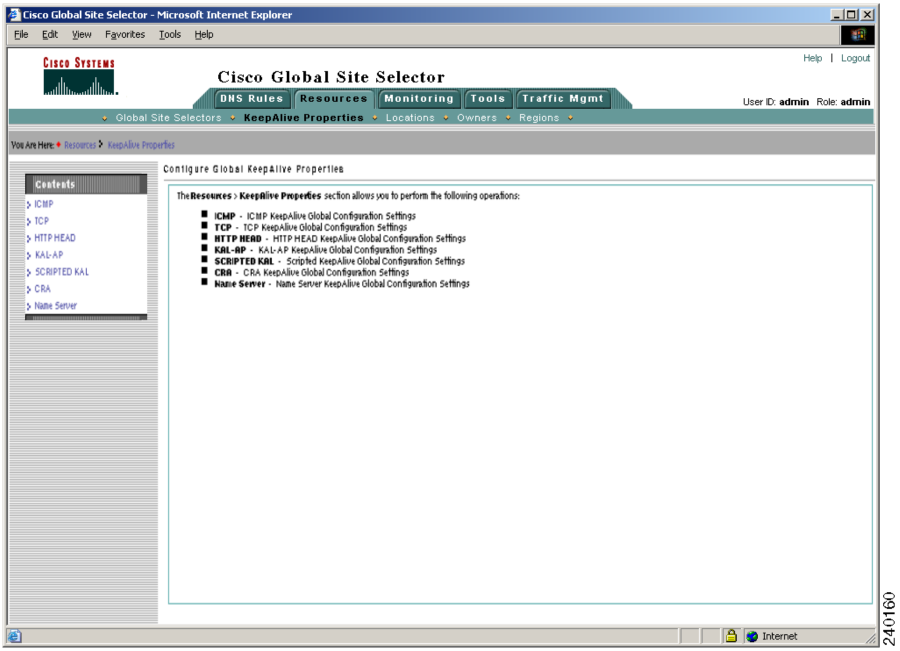
For example, if a VIP answer uses a TCP keepalive with all of its associated defaults, and you change the default port value from port 80 to port 23, port 23 automatically becomes the default for the TCP keepalive. If the GSS is transmitting numerous TCP keepalives using port 23, you should globally 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:

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 (Figure 5-1).

Figure 5-1 Configure Global KeepAlive Properties Details Page



Configure Global KeepAlive Properties

The **Resources** > **KeepAlive Properties** section allows you to perform the following operations:

- **ICMP** - ICMP KeepAlive Global Configuration Settings
- **TCP** - TCP KeepAlive Global Configuration Settings
- **HTTP HEAD** - HTTP HEAD KeepAlive Global Configuration Settings
- **KAL-AP** - KAL-AP KeepAlive Global Configuration Settings
- **SCRIPTED KAL** - Scripted KeepAlive Global Configuration Settings
- **CRA** - CRA KeepAlive Global Configuration Settings
- **Name Server** - Name Server KeepAlive Global Configuration Settings

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.

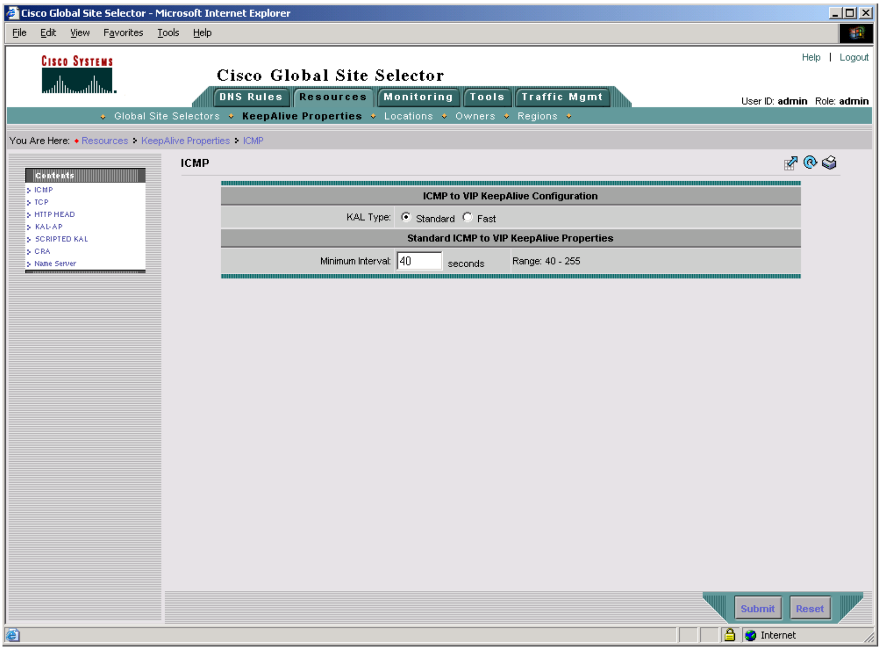
The following sections describe how to modify the default properties for the individual global keepalives.

- Modifying ICMP Global KeepAlive Settings
- Modifying TCP Global KeepAlive Settings
- Modifying HTTP HEAD Global KeepAlive Settings
- Modifying KAL-AP Global KeepAlive Settings
- Modifying Scripted KeepAlive Global KeepAlive Settings
- Modifying Name Server Global KeepAlive Settings

Modifying ICMP Global KeepAlive Settings

To modify the ICMP global keepalive configuration settings, perform the following procedure. Refer to Figure 5-2 and Figure 5-3 when performing this procedure.

Figure 5-2 ICMP Global KeepAlive—Standard KAL Type



ICMP to VIP KeepAlive Configuration

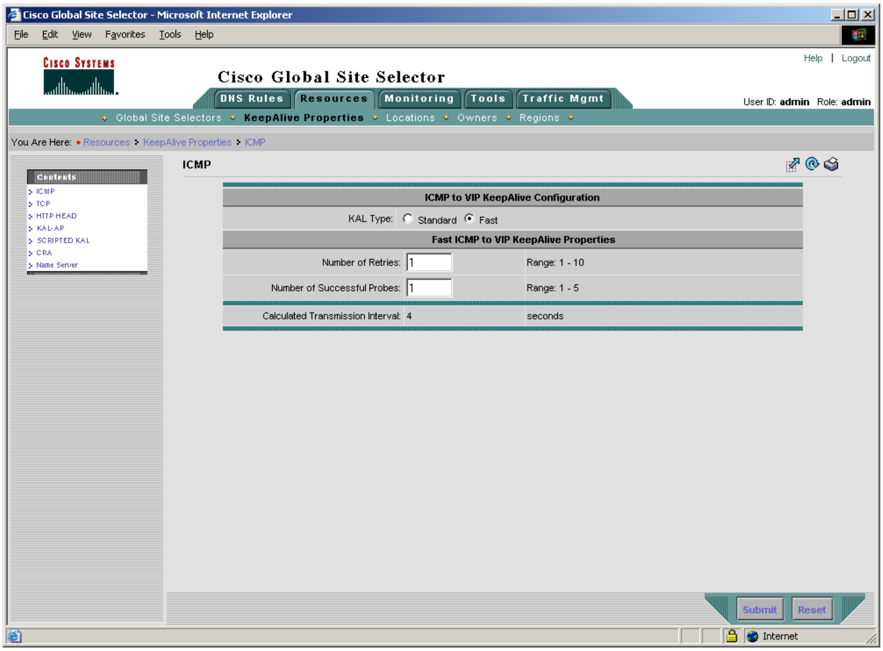
KAL Type: ● Standard ○ Fast

Standard ICMP to VIP KeepAlive Properties

Minimum Interval: 40 seconds Range: 40 - 255

240133

Figure 5-3 ICMP Global KeepAlive—Fast KAL Type



ICMP to VIP KeepAlive Configuration

KAL Type: ○ Standard ● Fast

Fast ICMP to VIP KeepAlive Properties

Number of Retries:	1	Range: 1 - 10
Number of Successful Probes:	1	Range: 1 - 5
Calculated Transmission Interval:	4	seconds

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. 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 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.

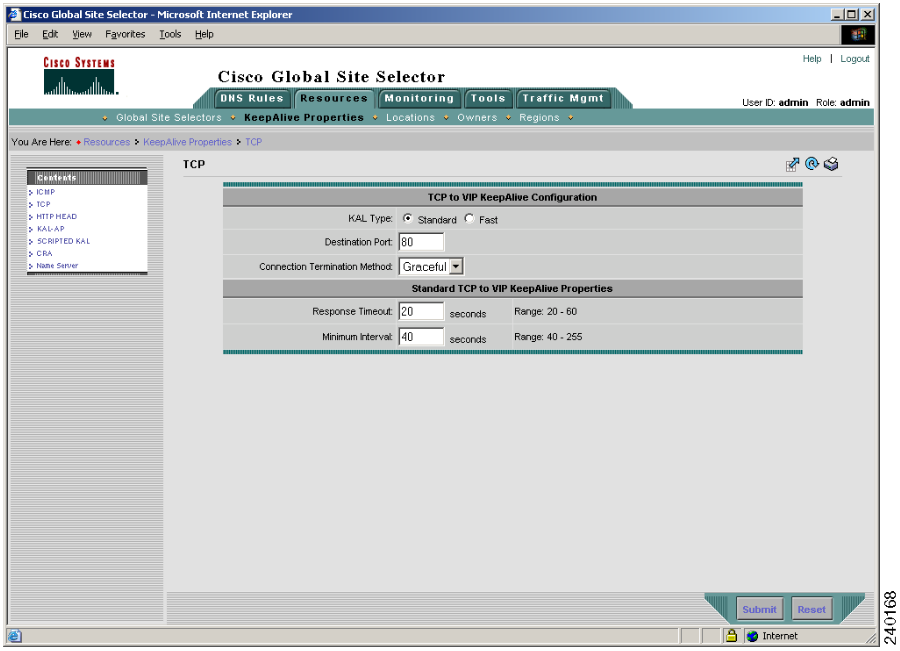
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 5-4 and Figure 5-5 when performing this procedure.

Figure 5-4 TCP Global KeepAlive—Standard KAL Type



TCP

TCP to VIP KeepAlive Configuration

KAL Type: ● Standard ○ Fast

Destination Port: 80

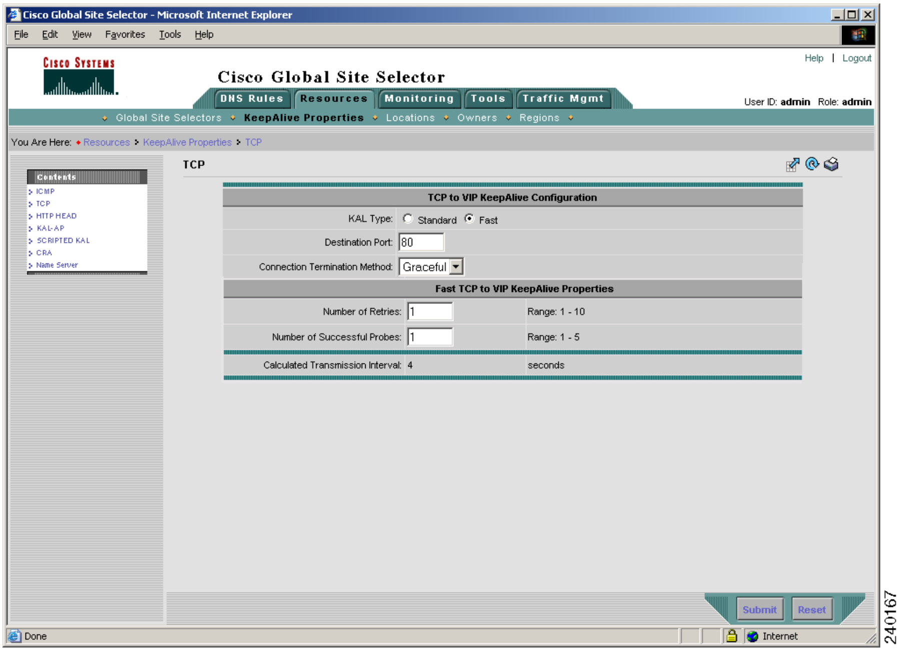
Connection Termination Method: Graceful

Standard TCP to VIP KeepAlive Properties

Response Timeout: 20 seconds Range: 20 - 60

Minimum Interval: 40 seconds Range: 40 - 255

Figure 5-5 TCP Global KeepAlive—Fast KAL Type


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors KeepAlive Properties Locations Owners Regions
You Are Here: Resources > KeepAlive Properties > TCP
Contents
ICMP
TCP
HTTP HEAD
KAL-AP
SCRIPTED KAL
CRA
Name Server
Submit
Reset
Done
Internet
240167

TCP

TCP to VIP KeepAlive Configuration

KAL Type: ○ Standard ● Fast

Destination Port: 80

Connection Termination Method: Graceful

Fast TCP to VIP KeepAlive Properties

Number of Retries: 1	Range: 1 - 10
Number of Successful Probes: 1	Range: 1 - 5
Calculated Transmission Interval: 4	seconds

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. 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.

      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.

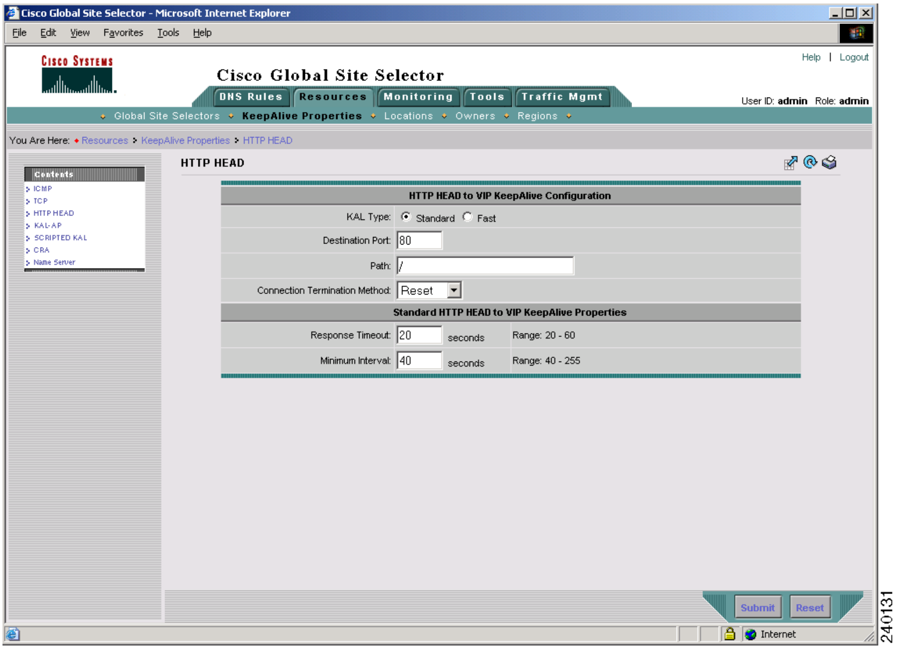
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 5-6 and Figure 5-7 when performing this procedure.

Figure 5-6 HTTP HEAD Global KeepAlive—Standard KAL Type



HTTP HEAD to VIP KeepAlive Configuration

KAL Type: ● Standard ○ Fast

Destination Port: 80

Path: /

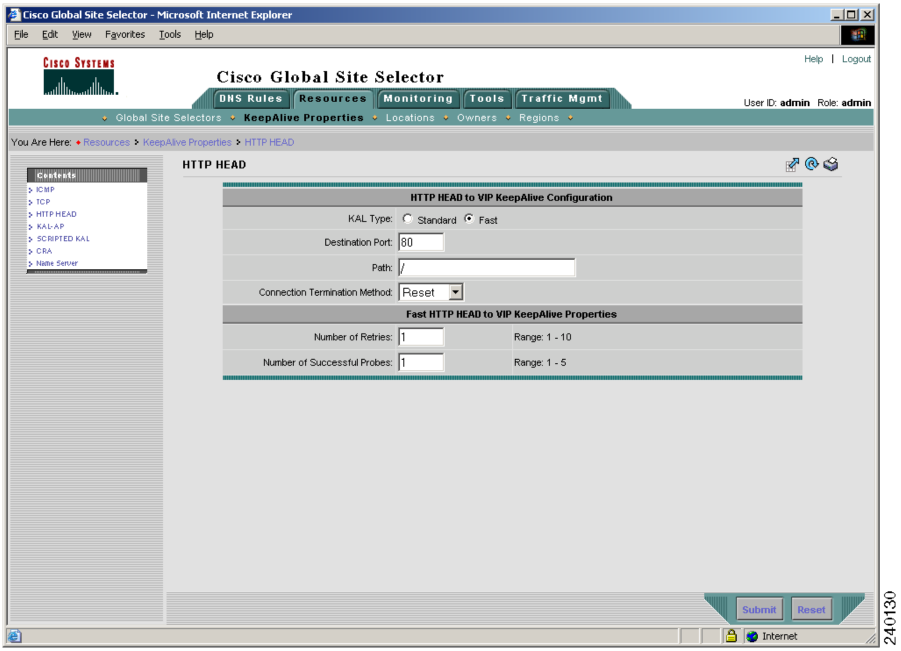
Connection Termination Method: Reset

Standard HTTP HEAD to VIP KeepAlive Properties

Response Timeout: 20 seconds Range: 20 - 60

Minimum Interval: 40 seconds Range: 40 - 255

Figure 5-7 HTTP HEAD Global KeepAlive—Fast KAL Type



HTTP HEAD to VIP KeepAlive Configuration

KAL Type: ○ Standard ● Fast

Destination Port: 80

Path: /

Connection Termination Method: Reset

Fast HTTP HEAD to VIP KeepAlive Properties

Number of Retries: 1 Range: 1 - 10

Number of Successful Probes: 1 Range: 1 - 5

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. 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.

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.

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 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.

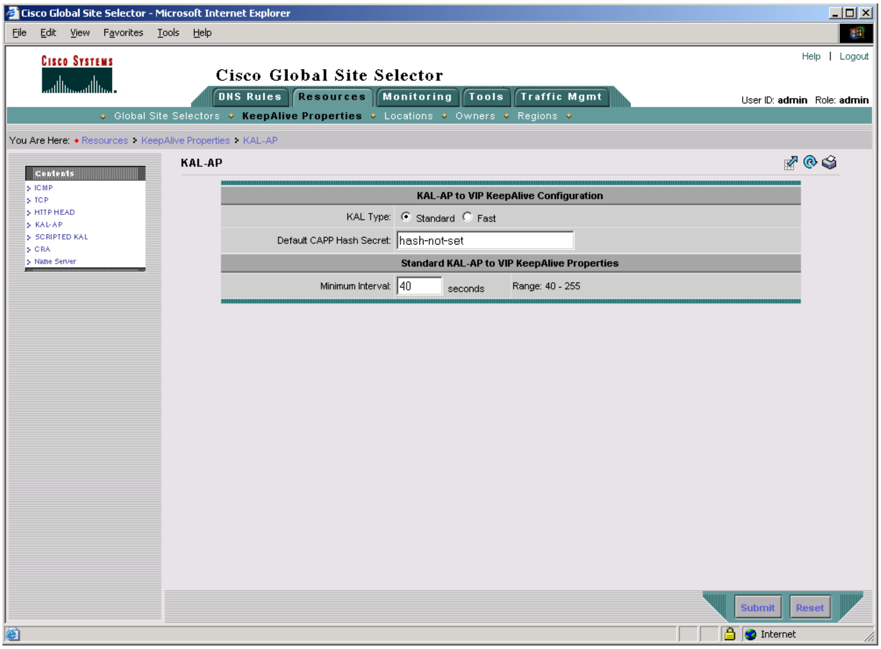
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

7. Click the **Submit** button to save your HTTP HEAD global keepalive modifications.

Modifying KAL-AP Global KeepAlive Settings

To modify the KAL-AP keepalive global configuration setting, perform the following procedure. Refer to Figure 5-8 and Figure 5-9 when performing this procedure.

Figure 5-8 KAL-AP Global KeepAlive—Standard KAL Type



Cisco Global Site Selector - Microsoft Internet Explorer

You Are Here: Resources > KeepAlive Properties > KAL-AP

KAL-AP

KAL-AP to VIP KeepAlive Configuration

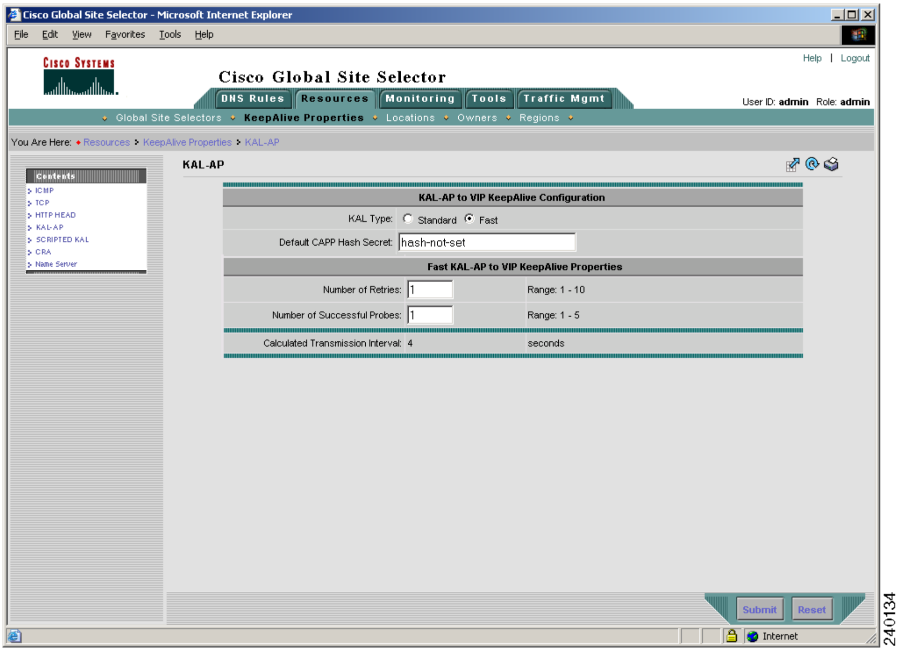
KAL Type: ● Standard ○ Fast

Default CAPP Hash Secret: hash-not-set

Standard KAL-AP to VIP KeepAlive Properties

Minimum Interval: 40 seconds Range: 40 - 255

Figure 5-9 KAL-AP Global KeepAlive—Fast KAL Type



KAL-AP to VIP KeepAlive Configuration

KAL Type: ○ Standard ● Fast

Default CAPP Hash Secret: hash-not-set

Fast KAL-AP to VIP KeepAlive Properties

Number of Retries:	1	Range: 1 - 10
Number of Successful Probes:	1	Range: 1 - 5
Calculated Transmission Interval:	4	seconds

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. 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 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.

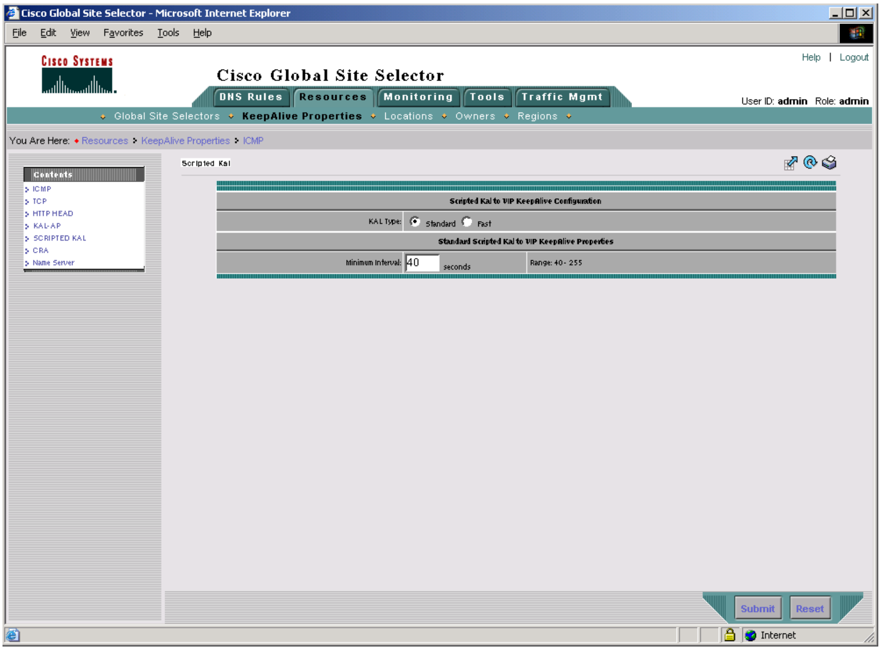
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 5-10 and Figure 5-11 when performing this procedure.

Figure 5-10 Scripted KAL Global KeepAlive—Standard KAL Type



Scripted Kal

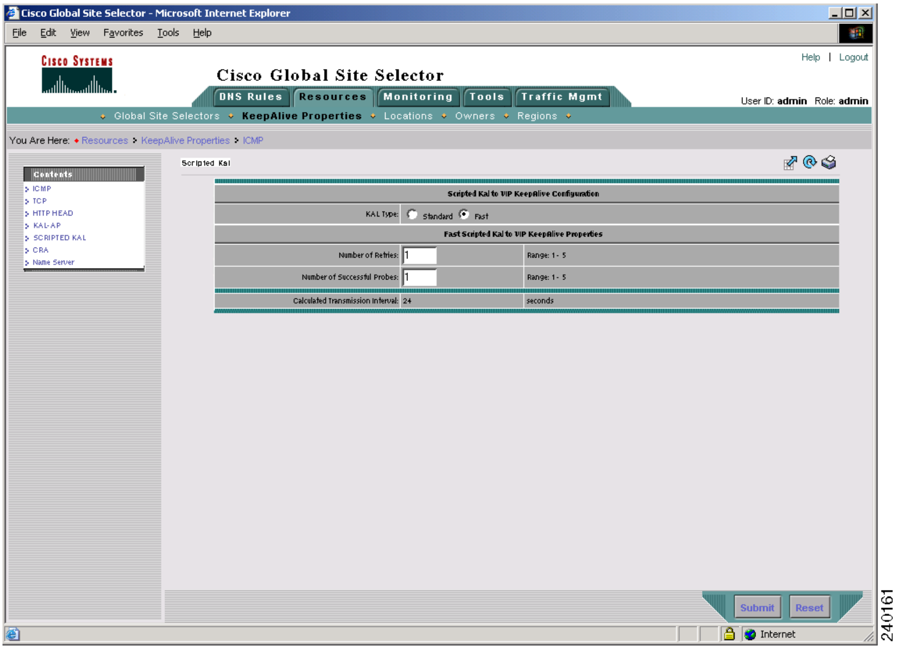
Scripted Kal to VIP KeepAlive Configuration

KAL Type: ● Standard ○ Fast

Standard Scripted Kal to VIP KeepAlive Properties

Minimum Interval: 40 seconds Range: 40 - 255

Figure 5-11 Scripted KAL Global KeepAlive—Fast KAL Type



Scripted Kal

Scripted Kal to VIP KeepAlive Configuration		
KAL Type:	○ Standard ● Fast	
Fast Scripted Kal to VIP KeepAlive Properties		
Number of Retries:	1	Range: 1 - 5
Number of Successful Probes:	1	Range: 1 - 5
Calculated Transmission Interval:	24	seconds

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. 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.

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 Kal 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 Kal 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.

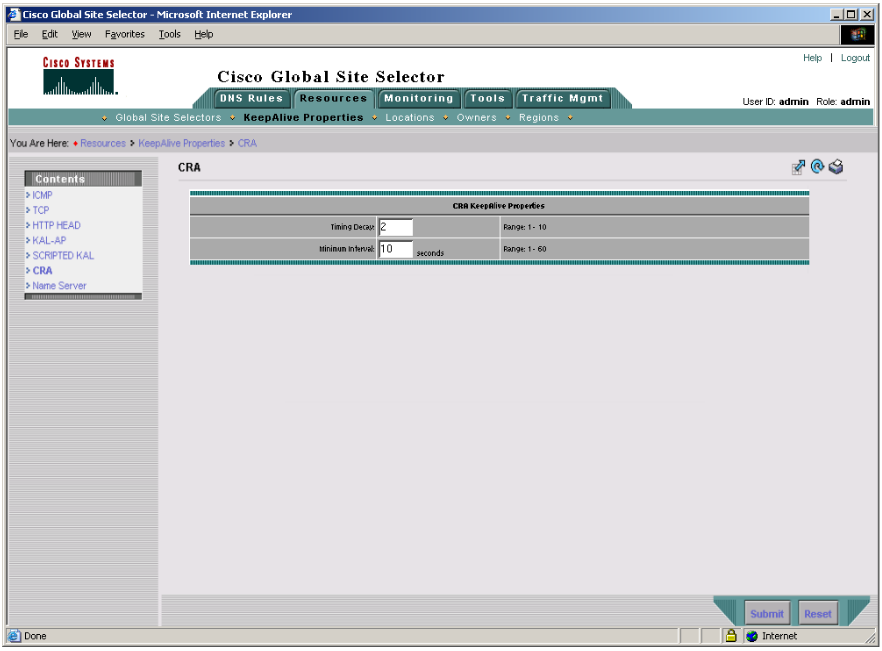
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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

Modifying CRA Global KeepAlive Settings

To modify the CRA keepalive global configuration settings, perform the following procedure. Refer to Figure 5-12 when performing this procedure.

Figure 5-12 Global KeepAlives Details Page—CRA KeepAlive



CRA

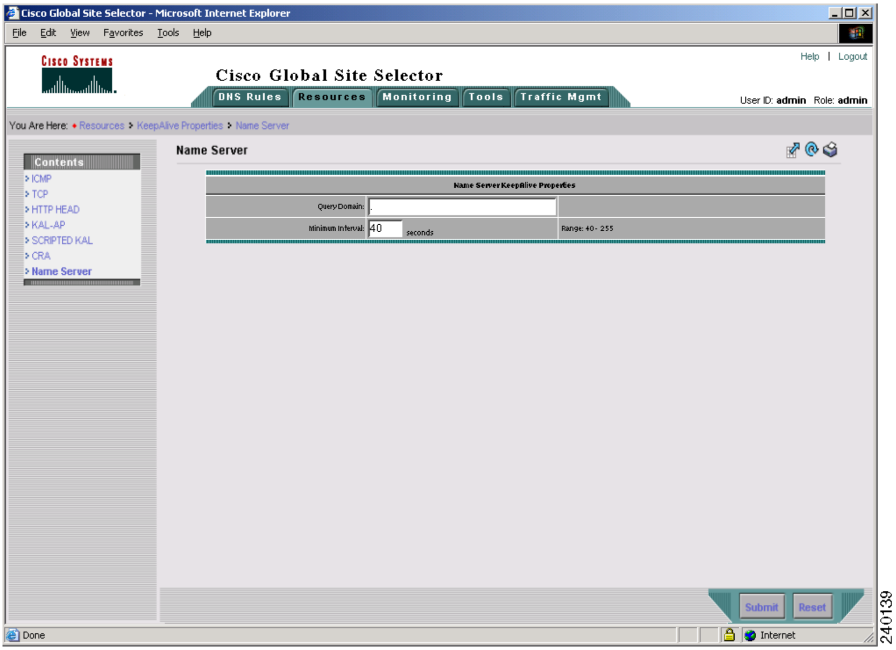
CRA KeepAlive Properties		
Timing Decay:	2	Range: 1 - 10
Minimum Interval:	10 seconds	Range: 1 - 60

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 procedure. Refer to Figure 5-13 when performing this procedure.

Figure 5-13 Global KeepAlives Details Page—Name Server KeepAlive


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
You Are Here: Resources > KeepAlive Properties > Name Server
Contents
ICMP
TCP
HTTP HEAD
KAL-AP
SCRIPTED KAL
CRA
Name Server
Submit
Reset
Done
Internet
240139

Name Server

Name Server KeepAlive Properties

Query Domain: .

Minimum Interval: 40 seconds Range: 40 - 255

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 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, and HTTP HEAD keepalive types.

This section includes the following procedures:

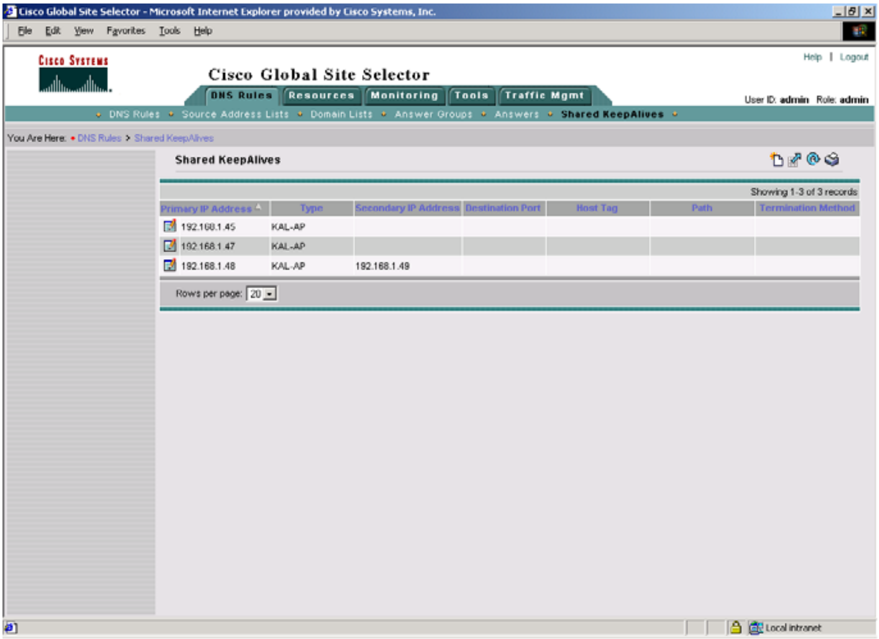
- Creating a Shared VIP KeepAlive
- Configuring Scripted KeepAlive Shared KeepAlive Configuration Settings
- Deleting a Shared KeepAlive

Creating a Shared VIP KeepAlive

To create a shared VIP keepalive:

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 (Figure 5-14).

Figure 5-14 Shared KeepAlives Lists Page



Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Cisco Global Site Selector

User ID: admin Role: admin

You Are Here: DNS Rules > Shared KeepAlives

Shared KeepAlives

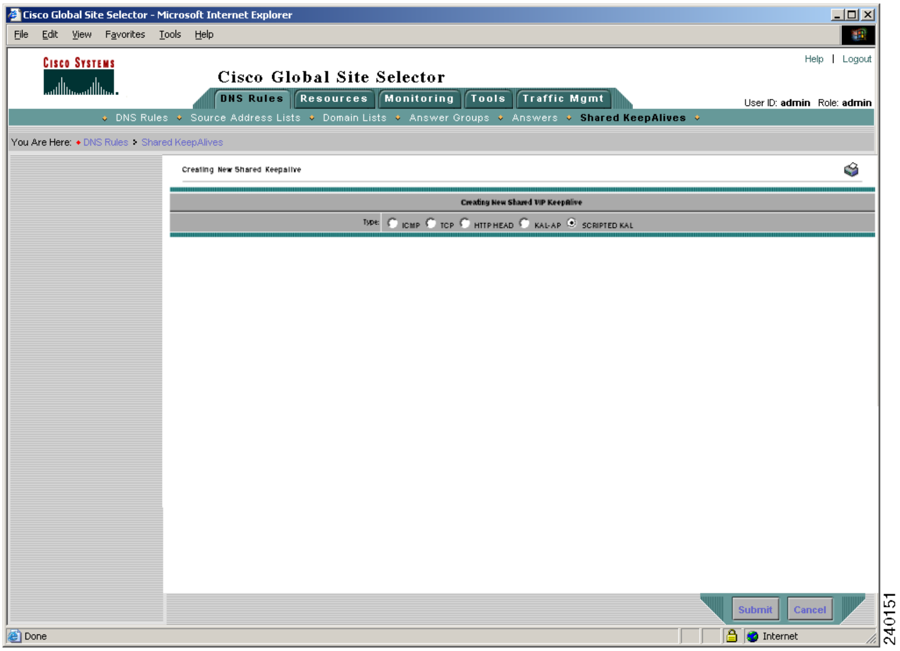
Showing 1-3 of 3 records

Primary IP Address	Type	Secondary IP Address	Destination Port	Host Tag	Path	Termination Method
192.168.1.45	KAL-AP					
192.168.1.47	KAL-AP					
192.168.1.48	KAL-AP	192.168.1.49				

Rows per page: 20

3. Click the **Create Shared KeepAlive** icon. The Creating New Shared KeepAlives details page appears (Figure 5-15).

Figure 5-15 Creating New Shared KeepAlives Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Shared KeepAlives
Submit
Cancel
Done
Internet
240151

Creating New Shared Keepalive

Creating New Shared VIP KeepAlive

Type: ○ ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ● SCRIPTED KAL

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, 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 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.

- **KAL-AP**—Sends a detailed query to the Cisco 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.

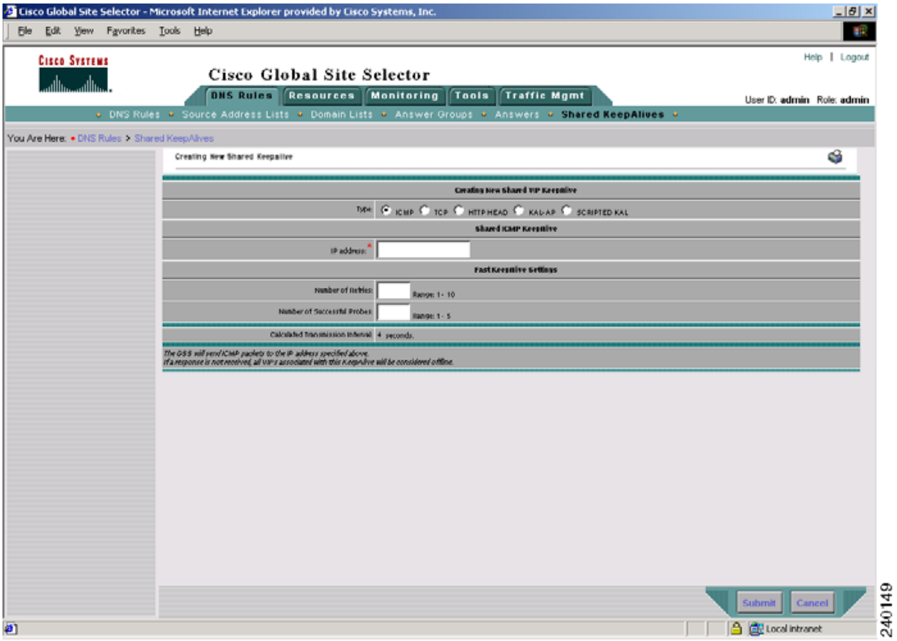
The following sections describe how to configure the properties for the individual VIP-shared keepalives. The default values used for each VIP keepalive is determined by the values specified in the Global Keepalive Properties details page.

- Configuring ICMP Shared KeepAlive Configuration Settings
- Configuring TCP Shared KeepAlive Configuration Settings
- Configuring HTTP HEAD Shared KeepAlive Configuration Settings
- Configuring KAL-AP Shared KeepAlive Configuration Settings
- Configuring Scripted KeepAlive Shared KeepAlive Configuration Settings

Configuring ICMP Shared KeepAlive Configuration Settings

To define the ICMP shared keepalive configuration, perform the following procedure. Refer to Figure 5-16 when performing this procedure.

Figure 5-16 Shared KeepAlives Details Page—ICMP KeepAlive (Fast KAL Type)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Shared KeepAlives
Submit
Cancel
Local intranet
240149

Creating New Shared Keepalive

Creating New Shared VIP Keepalive

Type: ● ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL

Shared ICMP Keepalive

IP address:*

Fast Keepalive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: 4 seconds.

The GSS will send ICMP packets to the IP address specified above.
If a response is not received, all VIP's associated with this KeepAlive will be considered offline.

1. Enter the IP address used to test the online status for the linked VIPs.

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.

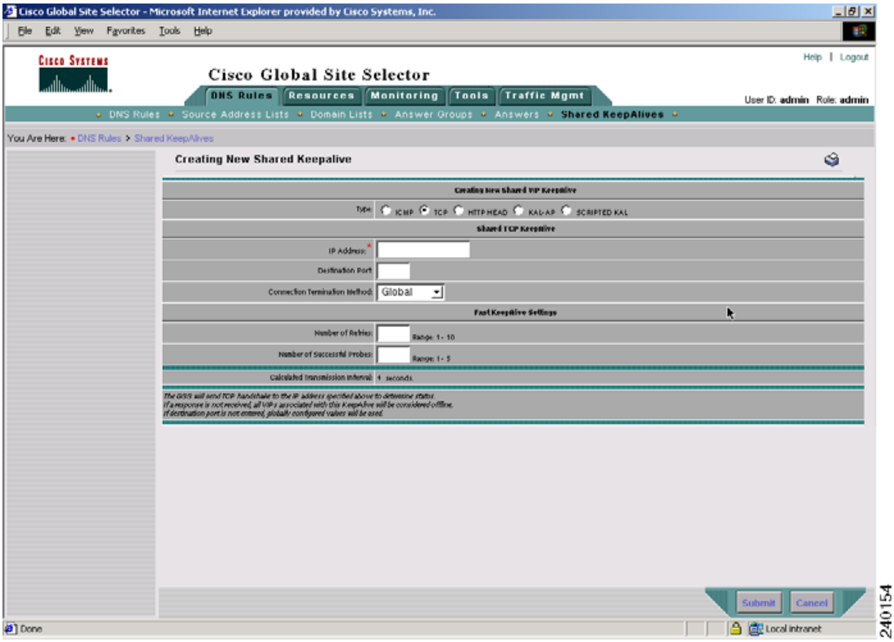
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 5-17 when performing this procedure.

Figure 5-17 Shared KeepAlives Details Page—TCP KeepAlive (Fast KAL Type)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules • Source Address Lists • Domain Lists • Answer Groups • Answers • Shared KeepAlives •
You Are Here: • DNS Rules > Shared KeepAlives
Submit Cancel
Done
Local intranet
240154

Creating New Shared Keepalive

Creating New Shared VIP Keepalive

Type: ○ ICMP ● TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL

Shared TCP Keepalive

IP Address:*

Destination Port

Connection Termination Method: Global

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated transmission interval: 4 seconds.

The GSS will send TCP handshake to the IP address specified above to determine status.
If a response is not received, all VIPs associated with this KeepAlive will be considered offline.
If destination port is not entered, globally configured values will be used.

1. Enter the IP address used to test the online status for the linked VIPs.

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.

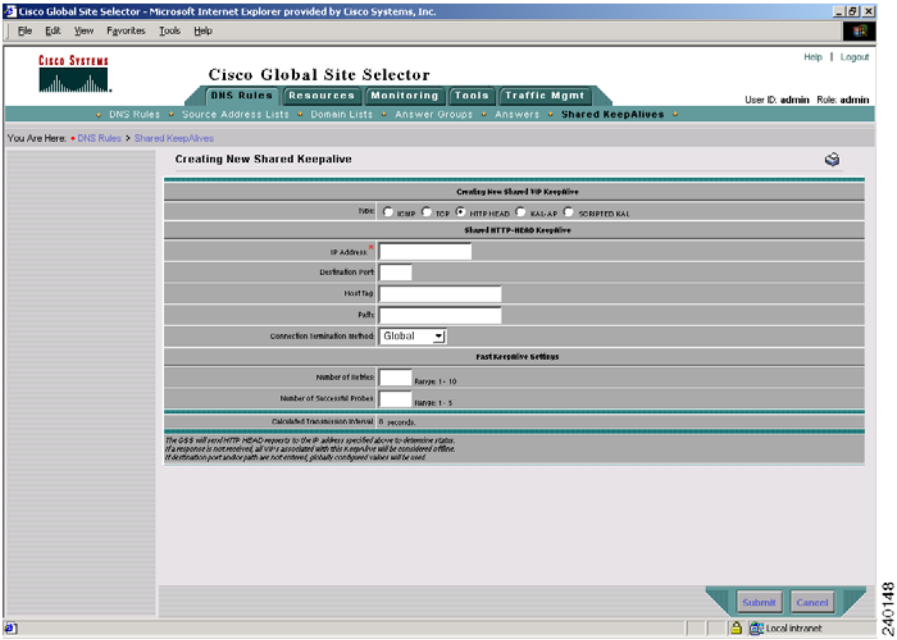
     Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

5. Click the **Submit** button to save your TCP-shared keepalive configuration and return to the Shared KeepAlives list page.

Configuring HTTP HEAD Shared KeepAlive Configuration Settings

To define the HTTP HEAD shared keepalive configuration, perform the following procedure. Refer to Figure 5-18 when performing this procedure.

Figure 5-18 Shared KeepAlives Details Page—HTTP HEAD KeepAlive (Fast KAL Type)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Shared KeepAlives
Submit
Cancel
Local intranet
240148

Creating New Shared Keepalive

Creating New Shared VIP KeepAlive

Type: ○ ICMP ○ TCP ● HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL

Shared HTTP-HEAD KeepAlive

IP Address: *

Destination Port:

Host Tag:

Path:

Connection Termination Method: Global

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: 0 seconds.

The GSS will send HTTP HEAD requests to the IP address specified above to determine status.
If a response is not received, all VIP's associated with this KeepAlive will be considered offline.
If destination port and/or path are not entered, globally configured values will be used.

1. Enter the IP address used to test the online status for the linked VIPs.
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:

   ```
   /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.

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.

   Note 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. If you do not specify a value, the GSS uses the globally configured value.

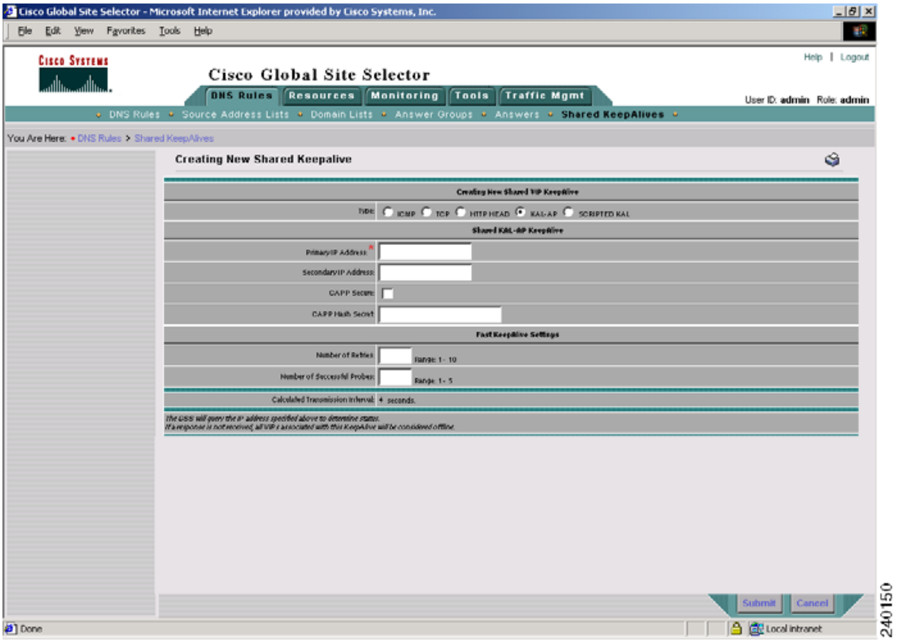
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

7. Click the **Submit** button to save your HTTP HEAD shared keepalive configuration and return to the Shared KeepAlives list page.

Configuring KAL-AP Shared KeepAlive Configuration Settings

To define the KAL-AP shared keepalive configuration, perform the following procedure. Refer to Figure 5-19 when performing this procedure.

Figure 5-19 Shared KeepAlives Details Page—KAL-AP KeepAlive (Fast KAL Type)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Shared KeepAlives
Submit
Cancel
Done
Local intranet
240150

Creating New Shared Keepalive

Creating New Shared VIP KeepAlive

Type: ○ ICMP ○ TCP ○ HTTP HEAD ● KAL-AP ○ SCRIPTED KAL

Shared KAL-AP KeepAlive

Primary IP Address: *

Secondary IP Address:

CAPP Secure: □

CAPP Hash Secret:

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: 4 seconds.

The GSS will query the IP address specified above to determine status.
If a response is not received, all VIPs associated with this KeepAlive will be considered offline.

1. Enter the primary (master) and secondary (backup) IP addresses that will be tested for the online status in the fields provided. The secondary IP address is optional. The purpose of the secondary IP address is to query a second Cisco CSS or CSM in a virtual IP (VIP) redundancy and virtual interface redundancy configuration.
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 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.

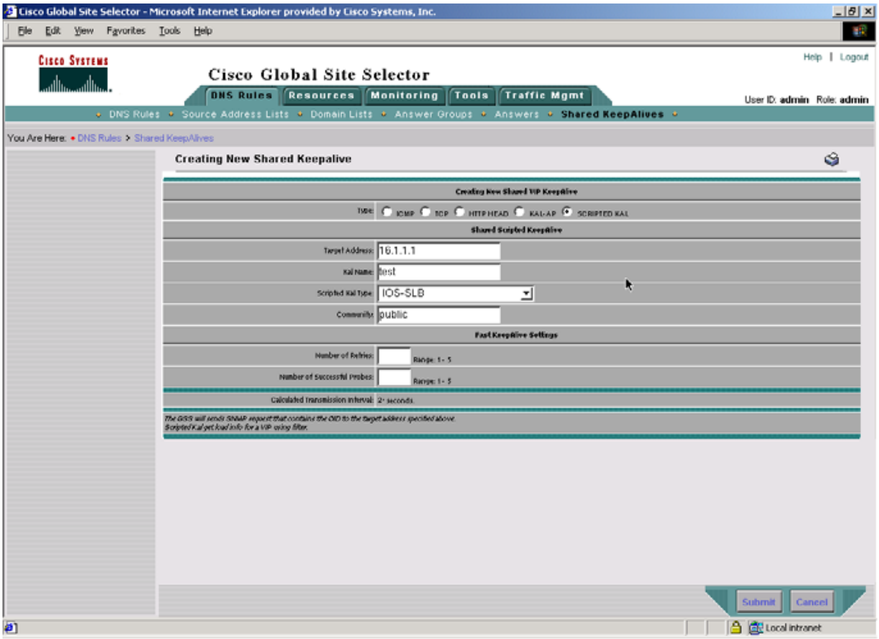
   Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 5-20 when performing this procedure.

Figure 5-20 Shared KeepAlives Details Page—SCRIPTED-KAL KeepAlive (Fast KAL Type)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules • Source Address Lists • Domain Lists • Answer Groups • Answers • Shared KeepAlives
You Are Here: • DNS Rules > Shared KeepAlives
Submit
Cancel
Local intranet
240152

Creating New Shared Keepalive

Creating New Shared VIP KeepAlive

Type: ○ ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ● SCRIPTED KAL

Shared Scripted KeepAlive

Target Address: 16.1.1.1

Kal Name: test

Scripted Kal Type: IOS-SLB

Community: public

Fast KeepAlive Settings

Number of Retries: Range: 1- 5

Number of Successful Probes: Range: 1- 5

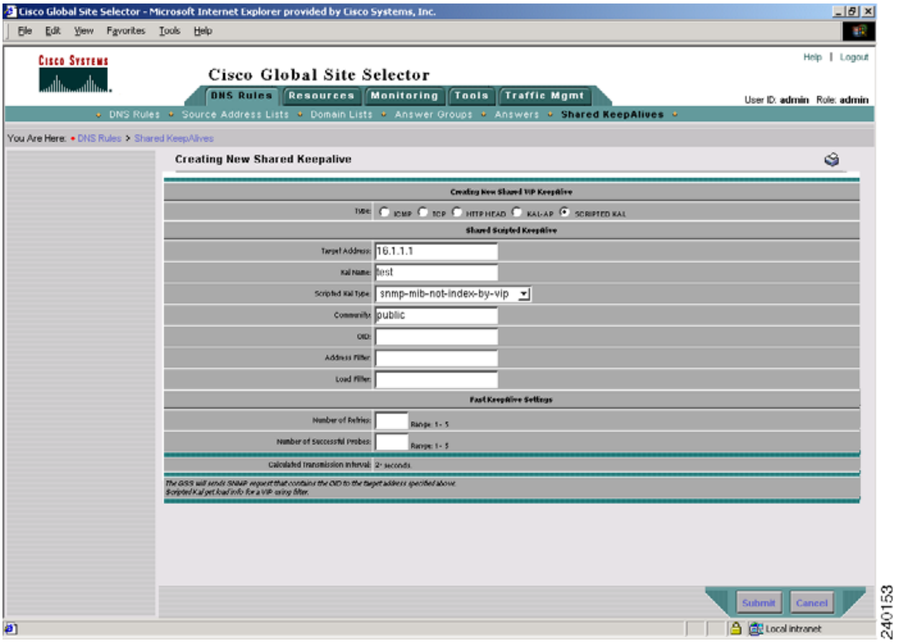
Calculated transmission interval: 2* seconds.

The GSS will sends SNMP request that contains the OID to the target address specified above.
Scripted Kal get load info for a VIP using filter.

1. Enter the target address that you wish to fetch load information from.
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.
4. Enter the Community. 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 OID and/or Address and Load filter types (Figure 5-21).

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

Figure 5-21 Shared KeepAlives Details Page—SCRIPTED-KAL KeepAlive (Non-Cisco SLB)


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: • DNS Rules > Shared KeepAlives
Submit
Cancel
Local intranet
240153

Creating New Shared Keepalive

Creating New Shared VIP KeepAlive

Type: ○ ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ● SCRIPTED KAL

Shared Scripted KeepAlive

Target Address: 16.1.1.1
Kal Name: test
Scripted Kal Type: snmp-mib-not-index-by-vip
Community: public
OID:
Address Filter:
Load Filter:

Fast KeepAlive Settings

Number of Retries: Range: 1- 5
Number of Successful Probes: Range: 1- 5
Calculated transmission interval: 2* seconds

The GSS will sends SNMP request that contains the OID to the target address specified above.
Scripted Kal get load info for a VIP using filter.

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

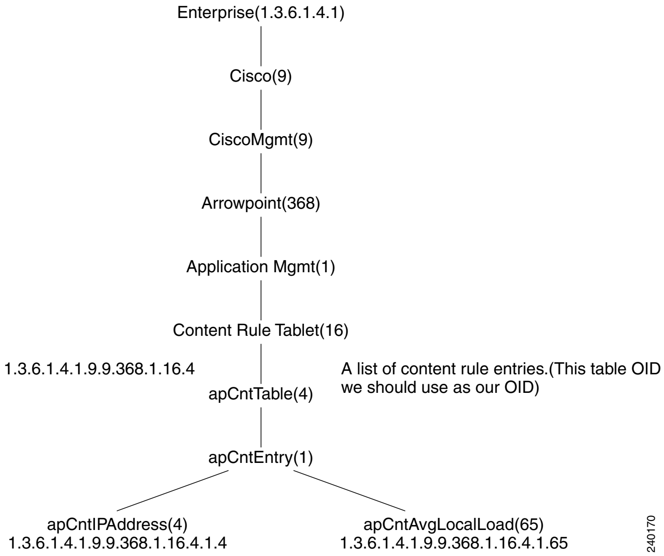
Device	Scripted Keepalive Types	OID	Address Filter	Load Filter	Recommended Software Version
CSS	CSS wrapper	*	*	*	**SLB**: 7.40.0.04
	SNMP_mib_not_index_by_vip	1.3.6.1.4.1.9.9.368.1.16.4	1.4	1.65	
CSM	CSM wrapper	*	*	*	**IOS**: 12.2
	SNMP_mib_not_index_by_vip	1.3.6.1.4.1.9.9.161.1.4.1	1.4	1.17	**CSM**: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

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

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

You can also configure Scripted keepalives with any OID that represents load information on an SLB. Depending on the type of table, that is whether the load information is scalar, indexed by VIP, or not indexed by VIP, address and load filters may be required. Figure 5-22 shows a configuration example using a CSS MIB tree.

Figure 5-22 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 5-22, you can see that the IP address of the pertinent VIP is referenced by the object apCntIPAddress (OID.1.4) and the load pertaining to this VIP is referenced by the object apCntAvgLocalLoad (OID.1.65). Thus, the IP address obtained here should populate the Address Filter, while the load information populates the Load Filter.

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

6. 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.

Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

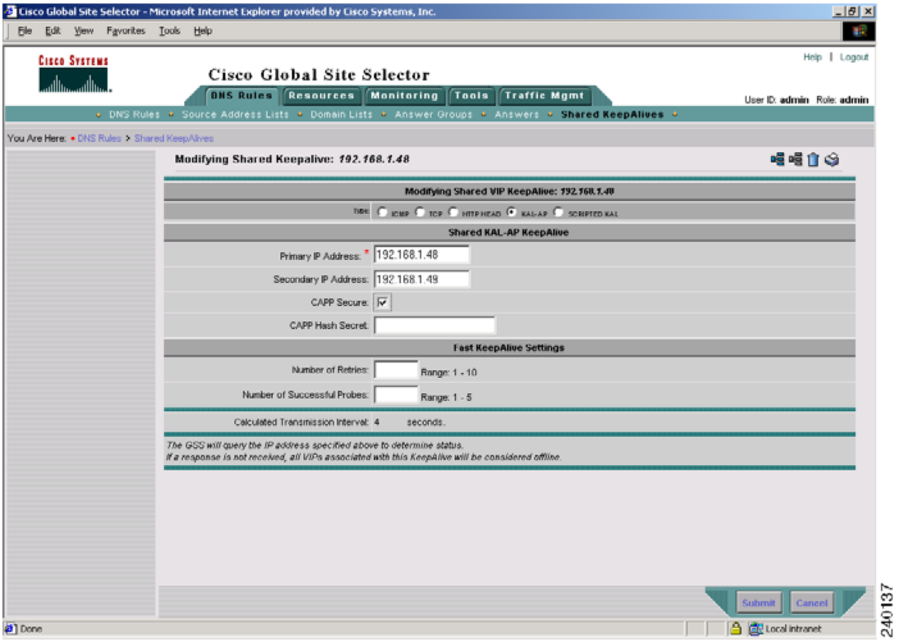
7. Click the **Submit** button to save your Scripted Kal shared keepalive configuration and return to the Shared KeepAlives list page.

Modifying a Shared KeepAlive

To modify an existing shared keepalive:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Shared KeepAlives** navigation link. The Shared KeepAlives list page appears (see Figure 5-14).
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 (Figure 5-23).

Figure 5-23 Modifying Shared KeepAlive Details Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules • Source Address Lists • Domain Lists • Answer Groups • Answers • Shared KeepAlives •
You Are Here: • DNS Rules > Shared KeepAlives
Submit Cancel
Done
Local intranet
240137

Modifying Shared Keepalive: *192.168.1.48*

Modifying Shared VIP KeepAlive: *192.168.1.48*

Type: ○ ICMP ○ TCP ○ HTTP HEAD ● KAL-AP ○ SCRIPTED KAL

Shared KAL-AP KeepAlive

Primary IP Address: * 192.168.1.48

Secondary IP Address: 192.168.1.49

CAPP Secure: ☑

CAPP Hash Secret:

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: 4 seconds.

The GSS will query the IP address specified above to determine status.
If a response is not received, all VIPs associated with this KeepAlive will be considered offline.

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. Refer to the *Global Site Selector Administration Guide* for details.

To delete a shared keepalive:

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, the term *answers* 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 that can provide the requesting client D-proxy with the address of a valid host to serve their request.

GSS answers include the following:

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

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

The GSS groups answers together as resource pools, also referred to as *answer groups*. From the available answer groups, the GSS can use 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.

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

This section includes the following procedures:

- 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-record containing the VIP of the SLB that manages the content.

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. Refer to Chapter 5, Configuring Keepalives for more information on creating shared keepalives.

The primary GSSM supports the assignment of multiple keepalives for a single VIP answer. You can configure up to five different keepalives for a VIP answer in a mix and match configuration of ICMP, TCP, HTTP HEAD, and KAL-AP VIP keepalive types. However, the primary GSSM supports only a single usage of a shared keepalive and a single KAL-AP keepalive when specifying multiple keepalive types.

For TCP or HTTP HEAD keepalives, you may also specify different destination ports. The multi-port keepalive capability allows you monitor a single server and check responses from multiple ports. As long as all the keepalives are successful, the GSS device considers the resource active and continues to redirect client traffic to the server. Servers that yield unsuccessful connections are marked as unavailable; subsequent successful connections to the server will reinstate it as available to be used as a resource.

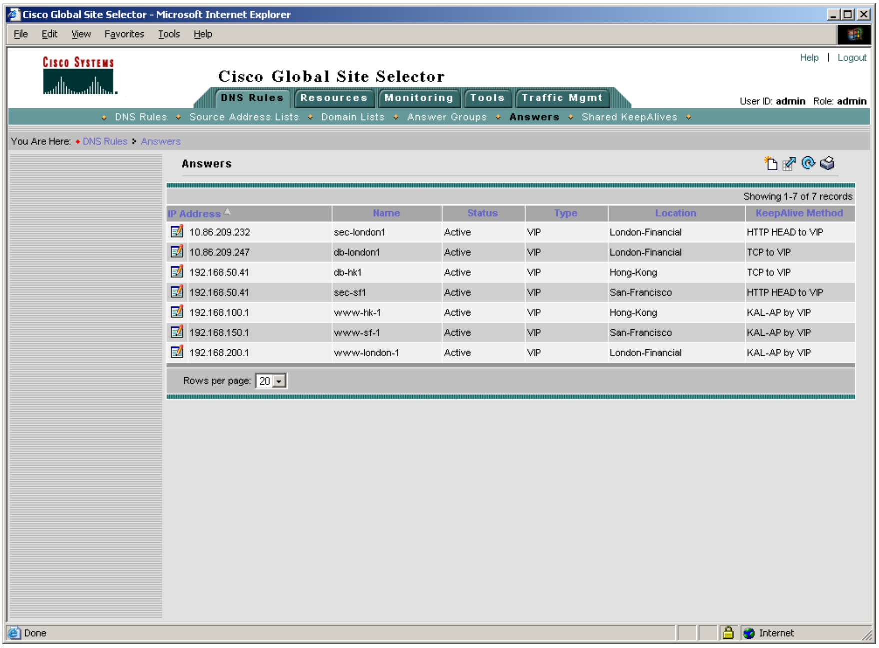
When using multiple keepalive types, the VIP answer status is a combination of all keepalive probes associated with an answer, resulting in a consolidation of results from each answer.

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

To configure a VIP-type answer:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (Figure 6-1).

Figure 6-1 Answers List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
User ID: admin Role: admin
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Answers
Done
Internet
148552

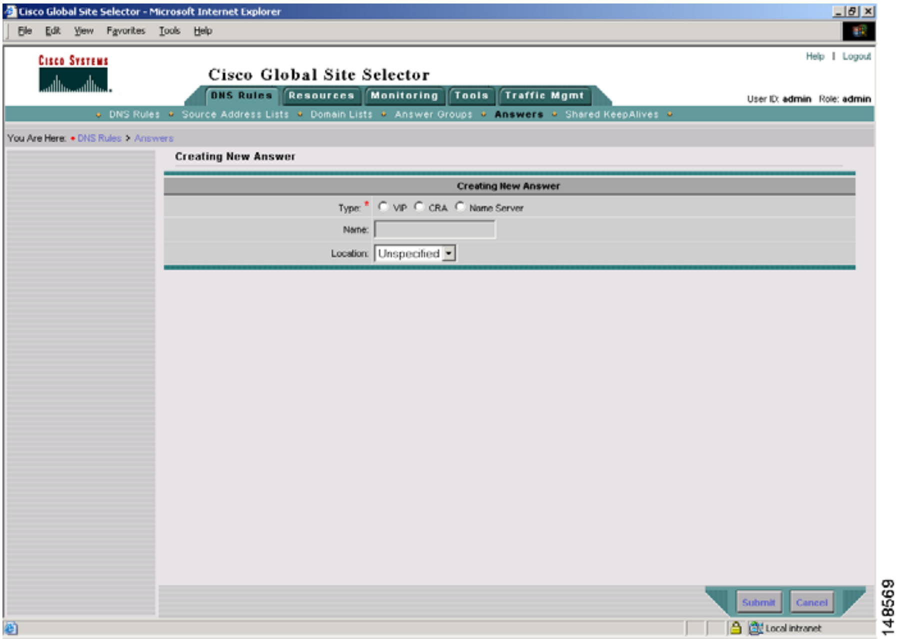
Showing 1-7 of 7 records

IP Address	Name	Status	Type	Location	KeepAlive Method
10.86.209.232	sec-london1	Active	VIP	London-Financial	HTTP HEAD to VIP
10.86.209.247	db-london1	Active	VIP	London-Financial	TCP to VIP
192.168.50.41	db-hk1	Active	VIP	Hong-Kong	TCP to VIP
192.168.50.41	sec-sf1	Active	VIP	San-Francisco	HTTP HEAD to VIP
192.168.100.1	www-hk-1	Active	VIP	Hong-Kong	KAL-AP by VIP
192.168.150.1	www-sf-1	Active	VIP	San-Francisco	KAL-AP by VIP
192.168.200.1	www-london-1	Active	VIP	London-Financial	KAL-AP by VIP

Rows per page: 20

3. Click the **Create Answer** icon. The Creating New Answer detail page appears (Figure 6-2).

Figure 6-2 Creating New Answer Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules • Source Address Lists • Domain Lists • Answer Groups • Answers • Shared KeepAlives
You Are Here: • DNS Rules > Answers
Submit
Cancel
Local intranet
148569

Creating New Answer

Creating New Answer

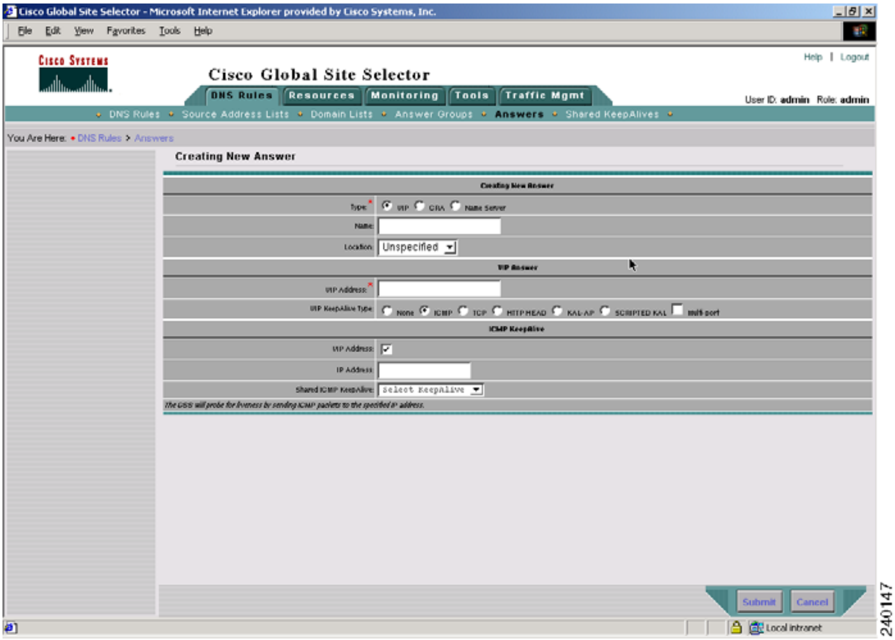
Type: * ○ VIP ○ CRA ○ Name Server

Name:

Location: Unspecified

4. In the Type field, click the **VIP** option button. The VIP Answer section appears in the details page (Figure 6-3).

Figure 6-3 Creating New Answer—VIP Details Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
Local intranet
240147

Creating New Answer

Creating New Answer

Type:* ● VIP ○ CRA ○ Name Server

Name:

Location: Unspecified

VIP Answer

VIP Address:*

VIP KeepAlive Type: ○ None ● ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL □ multi port

ICMP KeepAlive

VIP Address: ☑

IP Address:

Shared ICMP KeepAlive: Select KeepAlive

The GSS will probe for liveness by sending ICMP packets to the specified IP address.

5. In the Name field, enter a name for the VIP-type answer that you are creating. Specifying a name for an answer is an optional step.

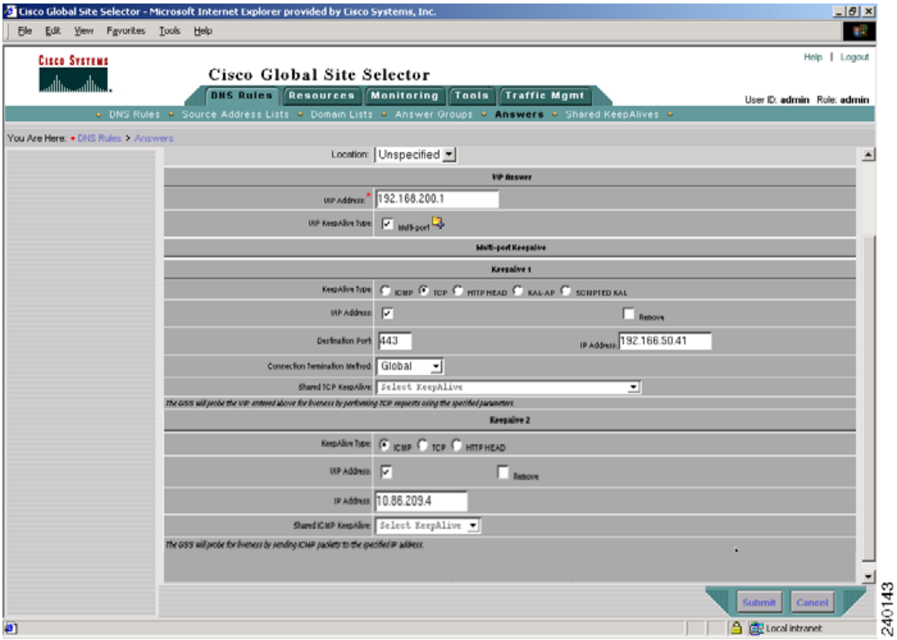
6. From the Location drop-down list, select a GSS location that corresponds to the answer. Specifying a location for an answer is an optional step unless you are assigning a location that is associated with a proximity zone to the answer. For details about creating a location, refer to Chapter 2, Configuring Resources.

7. In the VIP address field, enter the VIP address to which the GSS will forward requests.

8. In the VIP Keepalive section, click 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 (Figure 6-4).

Figure 6-4 Creating New Answer—Multi-port Keepalive Section


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
Local intranet
240143

Location: Unspecified

VIP Answer

VIP Address:* 192.168.200.1

VIP KeepAlive Type: ☑ Multi-port

Multi-port Keepalive

Keepalive 1

KeepAlive Type: ○ ICMP ● TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL

VIP Address: ☑ □ Remove

Destination Port: 443 IP Address: 192.166.50.41

Connection Termination Method: Global

Shared TCP KeepAlive: Select KeepAlive

The GSS will probe the VIP entered above for liveness by performing TCP requests using the specified parameters.

Keepalive 2

KeepAlive Type: ● ICMP ○ TCP ○ HTTP HEAD

VIP Address: ☑ □ Remove

IP Address: 10.86.209.4

Shared ICMP KeepAlive: Select KeepAlive

The GSS will probe for liveness by sending ICMP packets to the specified IP address.

The Multi-port Keepalive section includes:

- A VIP Address checkbox that selects either a shared or non-shared keepalive (checked selects a non-shared keepalive; unchecked selects a shared keepalive).
- An IP Address field that specifies the IP address of the device that is to be monitored by the keepalive. This field is accessible only when configuring non-shared keepalives (VIP Address checkbox must be checked)

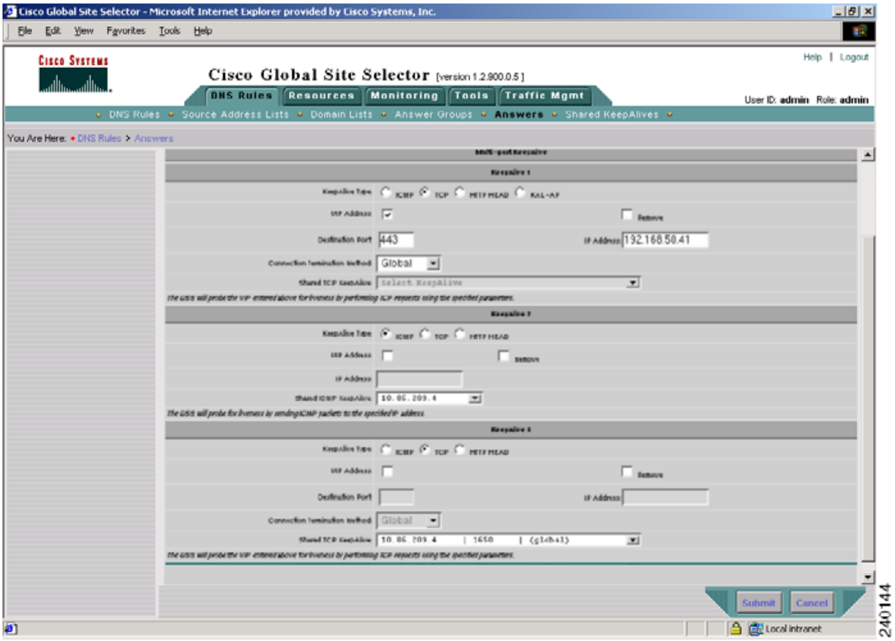
To add additional keepalives or destination ports for the VIP-type answer, click the **Multi-port** icon. The primary GSSM GUI adds a new numbered keepalive section to the bottom of the Creating New Answer details page.

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. Note that 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.

Figure 6-4 shows one non-shared TCP-type keepalive, while Figure 6-5 displays two shared keepalives (one ICMP-type and one TCP-type).

Figure 6-5 Creating New Answer Details Page with Two Keepalives


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector [version 1.2.900.0.5]
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
Local intranet
240144

Multi-port Keepalive

Keepalive 1

KeepAlive Type ○ ICMP ● TCP ○ HTTP HEAD ○ KAL-AP

VIP Address ☑ □ Remove

Destination Port 443 IP Address 192.168.50.41

Connection Termination Method Global

Shared TCP KeepAlive Select KeepAlive

The GSS will probe the VIP entered above for liveness by performing TCP requests using the specified parameters.

Keepalive 2

KeepAlive Type ● ICMP ○ TCP ○ HTTP HEAD

VIP Address □ □ Remove

IP Address

Shared ICMP KeepAlive 10.86.209.4

The GSS will probe for liveness by sending ICMP packets to the specified IP address.

Keepalive 3

KeepAlive Type ○ ICMP ● TCP ○ HTTP HEAD

VIP Address □ □ Remove

Destination Port IP Address

Connection Termination Method Global

Shared TCP KeepAlive 10.86.209.4 | 1650 | (global)

The GSS will probe the VIP entered above for liveness by performing TCP requests using the specified parameters.

9. Choose from one of these five 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.
- **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.
- **SCRIPTED-Kal**—Sends a detailed query that allows the GSS to use third-party applications to fetch load information from target devices.

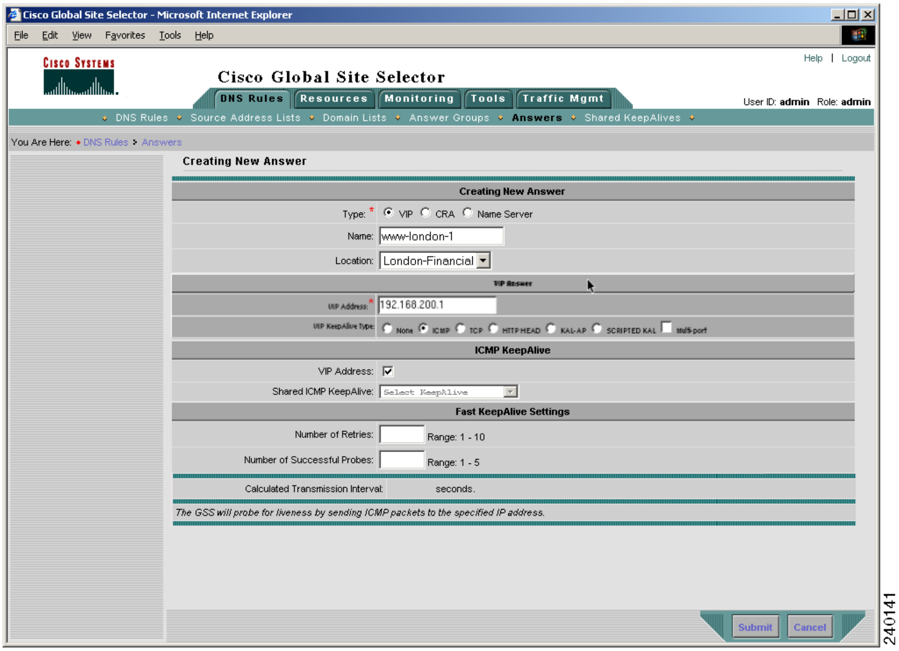
The following sections describe how to configure the properties for the individual VIP keepalives. The default values used for each of the VIP keepalives are determined by the values specified in the Global Keepalive Properties details page.

- Configuring ICMP Keepalive VIP Answer Settings
- Configuring TCP Keepalive VIP Answer Settings
- Configuring HTTP HEAD Keepalive VIP Answer Settings
- Configuring KAL-AP Keepalive VIP Answer Settings
- Configuring Scripted Kal Keepalive VIP Answer Settings

Configuring ICMP Keepalive VIP Answer Settings

To define the shared ICMP keepalive for your VIP answer, perform the following procedure. Refer to Figure 6-6 when performing this procedure (shown in single keepalive mode).

Figure 6-6 Answer Details Page—ICMP KeepAlive VIP Answer


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
240141

Creating New Answer

Creating New Answer

Type: * ● VIP ○ CRA ○ Name Server

Name: www-london-1

Location: London-Financial

VIP Answer

VIP Address: * 192.168.200.1

VIP KeepAlive Type: ○ None ● ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL □ Multi-port

ICMP KeepAlive

VIP Address: ☑

Shared ICMP KeepAlive: Select KeepAlive

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: seconds.

The GSS will probe for liveness by sending ICMP packets to the specified IP address.

1. If necessary, uncheck the VIP Address check box and select 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 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.

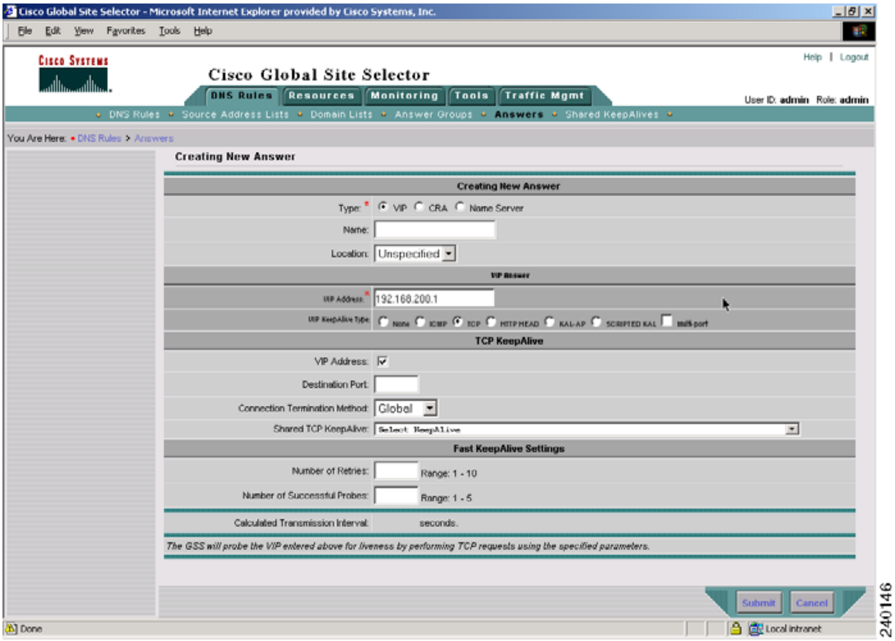
Note For more information on keepalive detection time, refer to Chapter 1, Introducing the Global Site Selector, the "Keepalives" section.

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 procedure. Refer to Figure 6-7 when performing this procedure (shown in single keepalive mode).

Figure 6-7 Answer Details Page—TCP KeepAlive VIP Answer


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
DNS Rules • Source Address Lists • Domain Lists • Answer Groups • Answers • Shared KeepAlives •
Submit
Cancel
Done
Local intranet
240146

User ID: admin Role: admin

You Are Here: • DNS Rules > Answers

Creating New Answer

Creating New Answer

Type:* ● VIP ○ CRA ○ Name Server

Name:

Location: Unspecified

VIP Answer

VIP Address:* 192.168.200.1

VIP KeepAlive Type: ○ None ○ ICMP ● TCP ○ HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL □ multi-port

TCP KeepAlive

VIP Address: ☑

Destination Port:

Connection Termination Method: Global

Shared TCP KeepAlive: Select KeepAlive

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: seconds.

The GSS will probe the VIP entered above for liveness by performing TCP requests using the specified parameters.

1. If necessary, 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, 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 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.

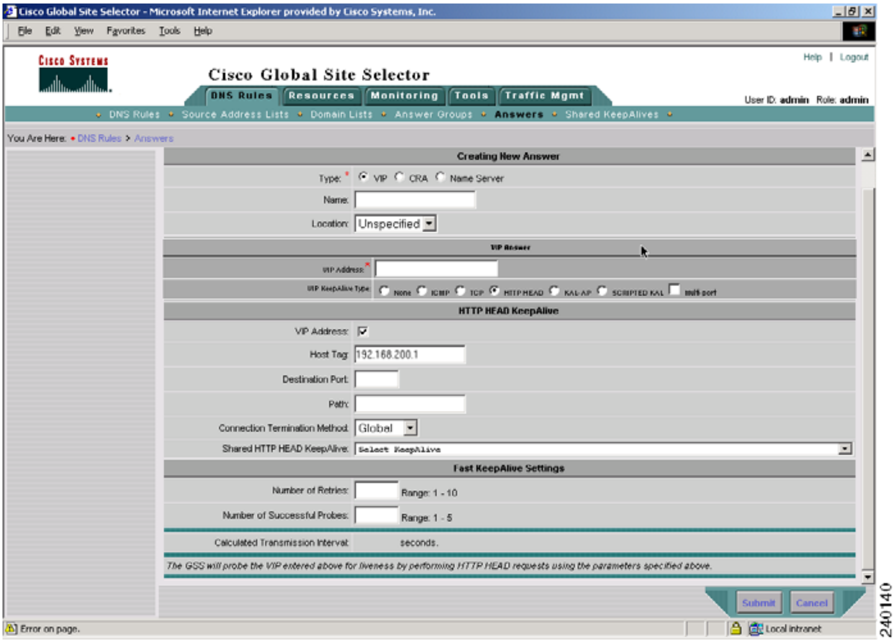
Note For more information on keepalive detection time, refer to the the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

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 procedure. Refer to Figure 6-8 when performing this procedure (shown in single keepalive mode).

Figure 6-8 Answer Details Page—HTTP HEAD KeepAlive VIP Answer



User ID: admin Role: admin

You Are Here: • DNS Rules > Answers

Creating New Answer

Type: * ● VIP ○ CRA ○ Name Server

Name:

Location: Unspecified

VIP Answer

VIP Address: *

VIP KeepAlive Type: ○ None ○ ICMP ○ TCP ● HTTP HEAD ○ KAL-AP ○ SCRIPTED KAL □ multi port

HTTP HEAD KeepAlive

VIP Address: ☑

Host Tag: 192.168.200.1

Destination Port:

Path:

Connection Termination Method: Global

Shared HTTP HEAD KeepAlive: Select KeepAlive

Fast KeepAlive Settings

Number of Retries: Range: 1 - 10

Number of Successful Probes: Range: 1 - 5

Calculated Transmission Interval: seconds.

The GSS will probe the VIP entered above for liveness by performing HTTP HEAD requests using the parameters specified above.

1. If necessary, uncheck the VIP Address check box and select 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: `/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, 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 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.

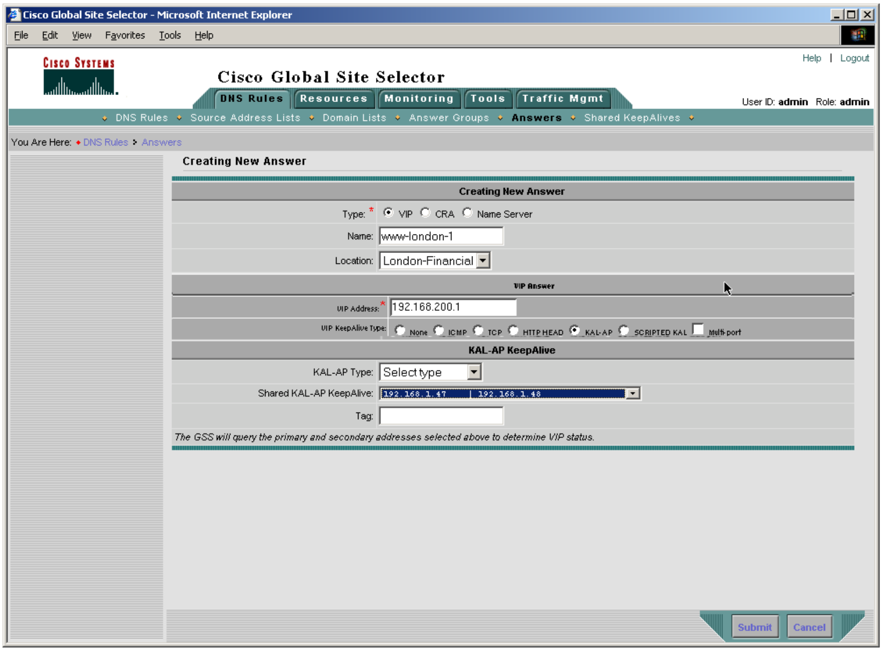
Note For more information on keepalive detection time, refer to the "Keepalives" section in Chapter 1, Introducing the Global Site Selector.

7. Click the **Submit** button to save your HTTP HEAD keepalive VIP answer and return to the Answers list page.

Configuring KAL-AP Keepalive VIP Answer Settings

To define the shared KAL-AP keepalive for your VIP answer, perform the following procedure. Refer to Figure 6-9 when performing this procedure (shown in single keepalive mode).

Figure 6-9 Answer Details Page—KAL-AP Keepalive VIP Answer


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
240142

Creating New Answer

Creating New Answer

Type: * ● VIP ○ CRA ○ Name Server

Name: www-london-1

Location: London-Financial

VIP Answer

VIP Address: * 192.168.200.1

VIP KeepAlive Type: ○ None ○ ICMP ○ TCP ○ HTTP HEAD ● KAL-AP ○ SCRIPTED KAL □ Multi-port

KAL-AP KeepAlive

KAL-AP Type: Select type

Shared KAL-AP KeepAlive: 192.168.1.47 | 192.168.1.48

Tag:

The GSS will query the primary and secondary addresses selected above to determine VIP status.

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).
   - **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 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 behavior typically occurs in situations where the GSS consumes the full datagram (roughly 1.4 K) with tag names or VIP addresses. Otherwise, all data fits perfectly in a single datagram.

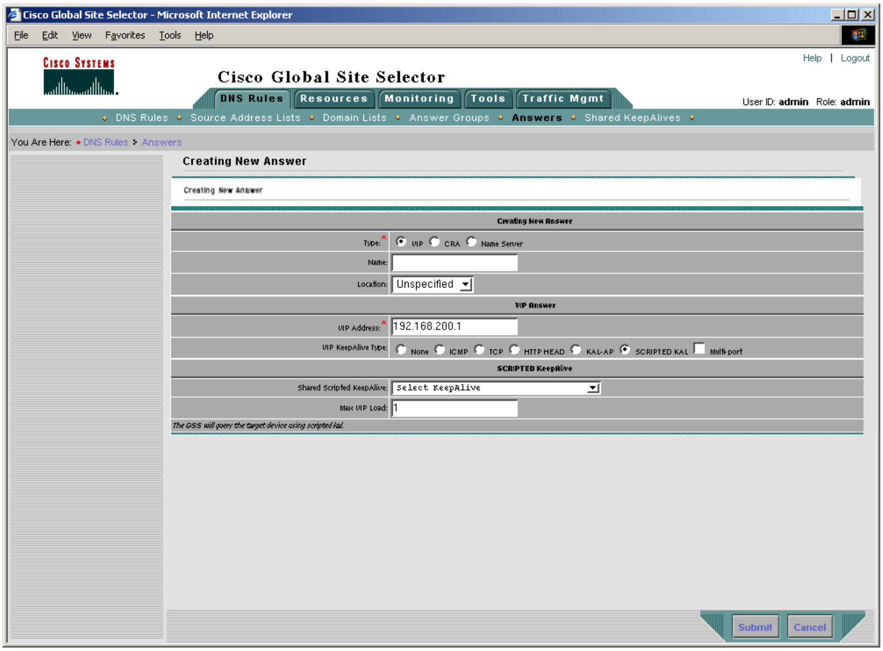
   To resolve this behavior, use the KAL-AP by VIP format when you need the GSS to send a detailed query on load for hundreds of VIPs configured to a single primary or optional secondary (backup) IP address. Another solution is to use the KAL-AP by Tag format, but to limit the length of Tag Names to ensure that the packets do not exceed 1.4K.

2. If you chose KAL-AP By VIP, select the appropriate KAL-AP type keepalive from the Shared KAL-AP Keepalive drop-down list.
3. If you chose KAL-AP By Tag, select the appropriate KAL-AP type keepalive from the Shared KAL-AP Keepalive drop-down list, 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 Kal Keepalive VIP Answer Settings

To define the shared Scripted Kal keepalive for your VIP answer, perform the following procedure. Refer to Figure 6-10 when performing this procedure (shown in single keepalive mode).

Figure 6-10 Answer Details Page—Scripted Kal KeepAlive VIP Answer


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
240145

Creating New Answer

Creating New Answer

Creating New Answer	
Type:*	● VIP ○ CRA ○ Name Server
Name:	
Location:	Unspecified
VIP Answer	
VIP Address:*	192.168.200.1
VIP KeepAlive Type:	○ None ○ ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP ● SCRIPTED KAL □ Multi-port
SCRIPTED KeepAlive	
Shared Scripted KeepAlive:	Select KeepAlive
Max VIP Load:	1

The GSS will query the target device using scripted kal.

1. From the Shared Scripted Kal KeepAlive drop-down list, select the Scripted Kal you wish.
2. Enter the Max VIP load.

Note For more information on keepalive detection time, refer to Chapter 1, Introducing the Global Site Selector, the "Keepalives" section.

3. Click the **Submit** button to save your Scripted Kal 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).

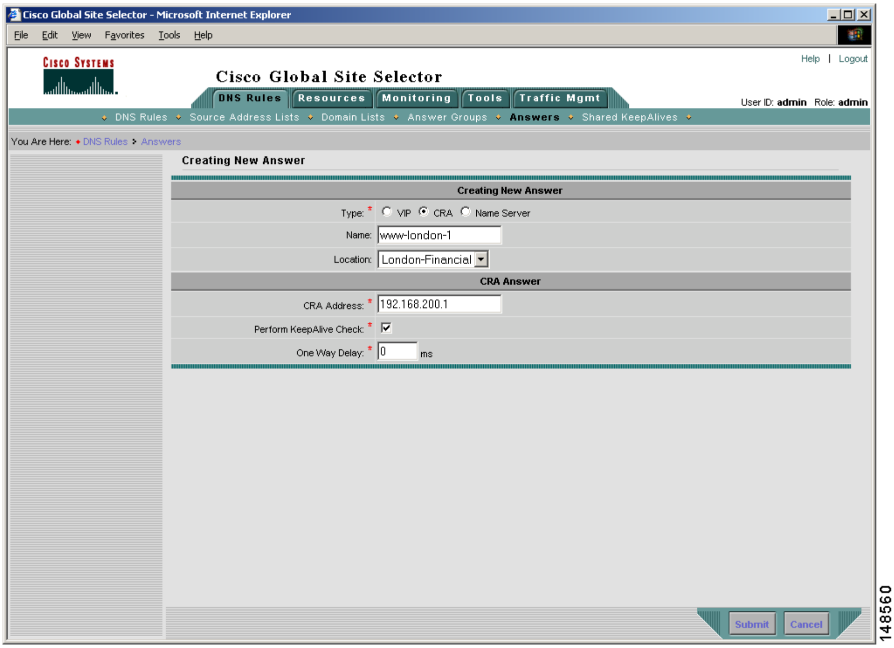
Closeness is determined when multiple hosts reply to the requesting D-proxy simultaneously in what is referred to as a "DNS race." The GSS coordinates the start of the race so that all CRAs initiate their response at the same time. The first DNS reply to reach the D-proxy is chosen by the name server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

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

To configure a CRA-type answer type:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (see Figure 6-1).
3. Click the **Create Answer** icon. The Creating New Answer details page appears (see Figure 6-2).
4. In the Type selection field, click the **CRA** option button. The CRA Answer section appears in the details page (Figure 6-11).

Figure 6-11 Creating New Answer—CRA Answer


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
148560

Creating New Answer

Creating New Answer

Type: * ○ VIP ● CRA ○ Name Server

Name: www-london-1

Location: London-Financial

CRA Answer

CRA Address: * 192.168.200.1

Perform KeepAlive Check: * ☑

One Way Delay: * 0 ms

5. In the Name field, enter a name for the CRA-type answer. Specifying a name for an answer is an optional step.
6. In the Location drop-down list, select a location for the answer. Specifying a location for an answer is an optional step. For details about creating a location, refer to Chapter 2, Configuring Resources.

7. In the CRA Address field, enter the interface or circuit address of the CRA.
8. 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.
9. 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.
10. Click **Submit** to create your new CRA-type answer and return to the Answers list page.

Creating a Name Server-Type Answer

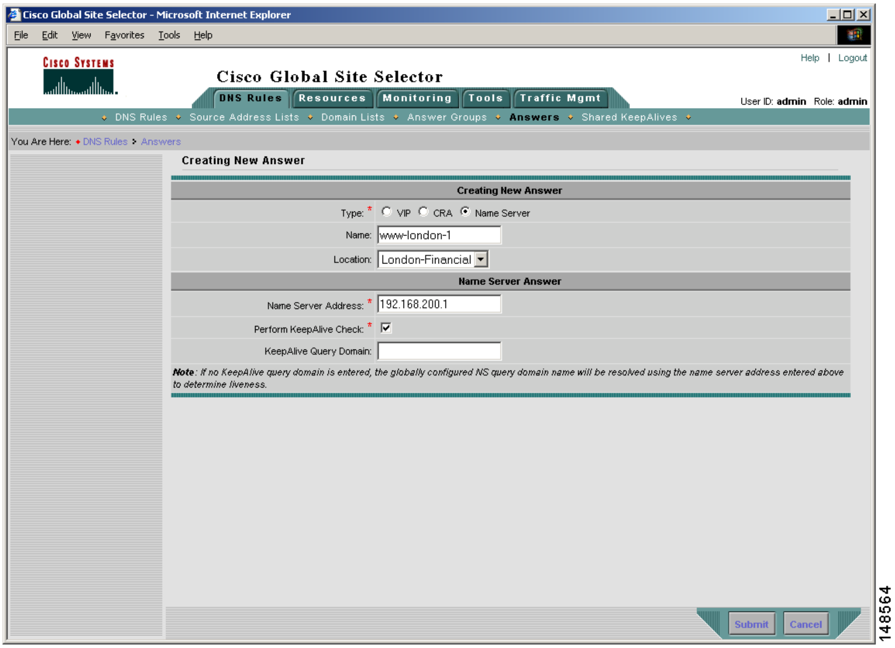
A name server (NS)-type answer specifies the IP address of a DNS name server to which DNS queries are forwarded from the GSS. Using the name server forwarding feature, queries are forwarded to a non-GSS name server for resolution, with the answer passed back to the GSS name server and from there to the 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).

To configure a name server-type answer:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (see Figure 6-1).
3. Click the **Create Answer** icon. The Creating New Answer details page appears (see Figure 6-2).
4. In the Type field, click the **Name Server** option button. The Name Server Answer section appears in the Creating New Answer details page (Figure 6-12).

Figure 6-12 Creating New Answer—Name Server Answer


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
148564

Creating New Answer

Type: *	○ VIP ○ CRA ● Name Server
Name:	www-london-1
Location:	London-Financial

Name Server Answer

Name Server Address: *	192.168.200.1
Perform KeepAlive Check: *	☑
KeepAlive Query Domain:	

***Note**: If no KeepAlive query domain is entered, the globally configured NS query domain name will be resolved using the name server address entered above to determine liveness.*

5. In the Name field, enter a name for the name server-type answer. Specifying a name for an answer is an optional step.

6. From the Location drop-down list, select a GSS location to which the answer corresponds. Specifying a location for an answer is an optional step. For details about creating a location, refer to Chapter 2, Configuring Resources.

7. In the Name Server Address field, enter the IP address of the name server that the GSS is to forward its requests.

8. 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.

9. If you wish 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.

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

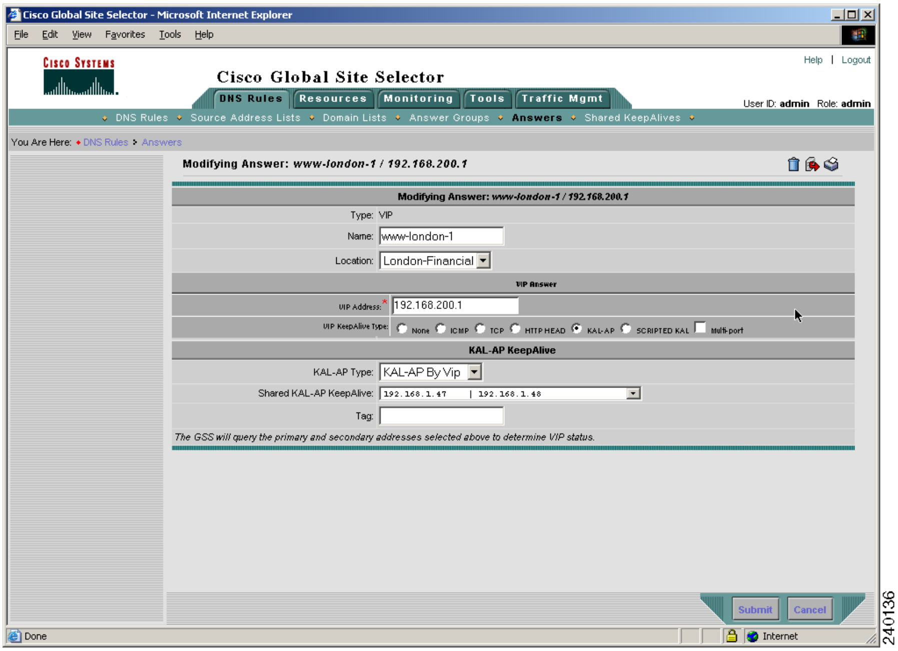
Modifying an Answer

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).

To modify an existing answer:

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 (Figure 6-13).

Figure 6-13 Modifying Answer Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Help | Logout
Cisco Systems
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
Done
Internet
240136

Modifying Answer: *www-london-1 / 192.168.200.1*

Type:	VIP
Name:	www-london-1
Location:	London-Financial

VIP Answer

VIP Address:*	192.168.200.1
VIP KeepAlive Type:	○ None ○ ICMP ○ TCP ○ HTTP HEAD ● KAL-AP ○ SCRIPTED KAL □ Multi-port

KAL-AP KeepAlive

KAL-AP Type:	KAL-AP By Vip
Shared KAL-AP KeepAlive:	192.168.1.47 | 192.168.1.48
Tag:	

The GSS will query the primary and secondary addresses selected above to determine VIP status.

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 to prevent 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:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (see Figure 6-1).
3. Click the **Modify Answer** icon located to the left of the answer you want to suspend. The Modifying Answer details page appears (see Figure 6-13).
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:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (see Figure 6-1).
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 (see Figure 6-13).
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

Answers can be grouped and managed 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 the purposes of software upgrades or regular maintenance.

The GSS automatically detects and routes requests around suspended answers. 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:

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 suspended answers associated with this location, click the **Activate All Answers in This Location** icon.
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 wish 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. Refer to the *Global Site Selector Administration Guide* for details.

To delete an answer:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answers** navigation link. The Answers list page appears (see Figure 6-1).
3. Click the **Modify Answer** icon located to the left of the answer you want to remove. The Modifying Answer details page appears (see Figure 6-13).
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.

- 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 includes the following procedures:

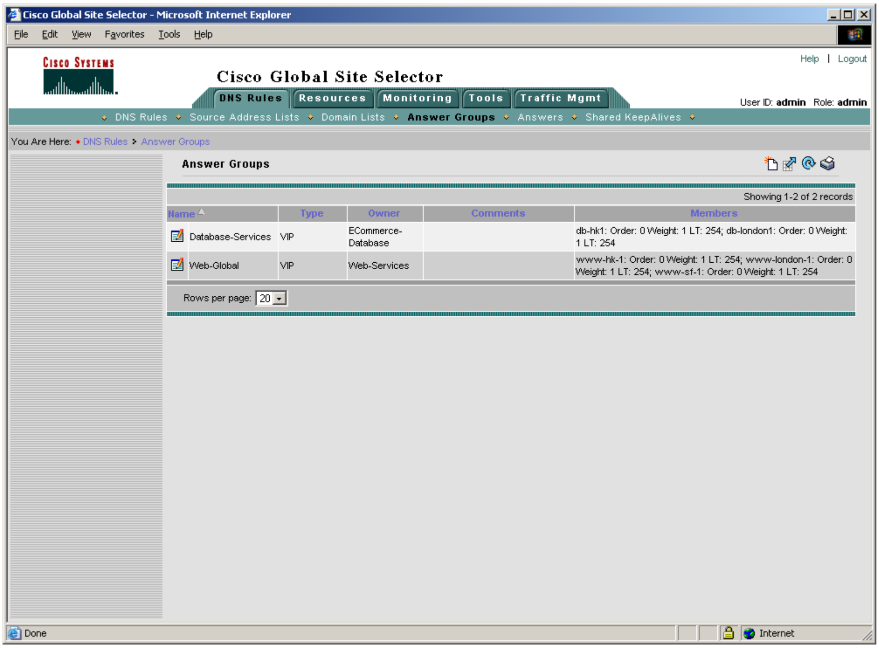
- Creating an Answer Group
- Modifying an Answer Group
- Configuring an Authority Domain for an Answer Group
- Deleting an Authority Domain for an Answer Group
- Suspending or Reactivating Answers in an Answer Group
- Suspending or Reactivating All Answers in an Answer Group Associated with an Owner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

Creating an Answer Group

You can configure up to 1000 answer groups on the primary GSSM. To create an answer group:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears (Figure 6-14).

Figure 6-14 Answer Group List Page



Answer Groups

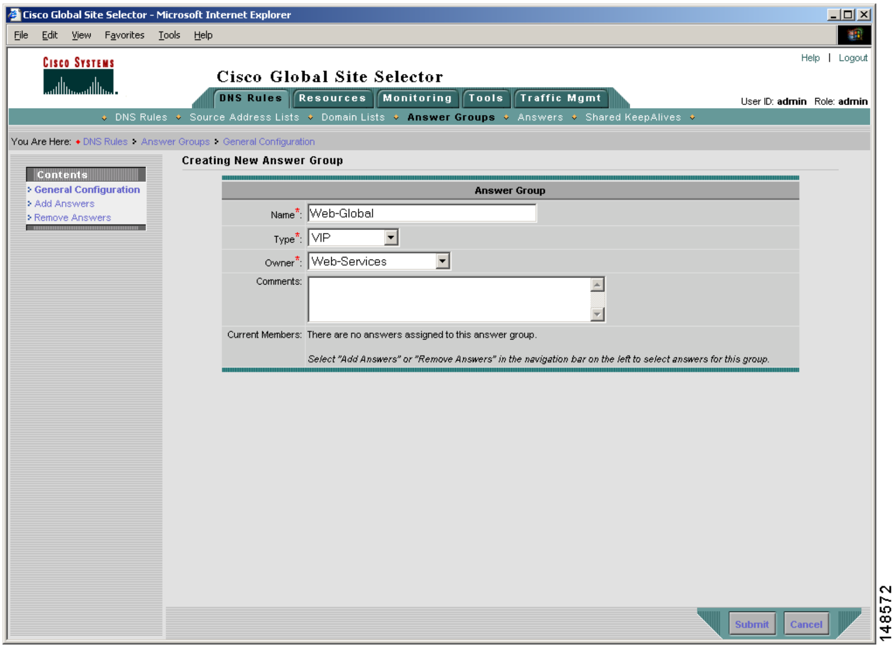
Showing 1-2 of 2 records

Name	Type	Owner	Comments	Members
Database-Services	VIP	ECommerce-Database		db-hk1: Order: 0 Weight: 1 LT: 254; db-london1: Order: 0 Weight: 1 LT: 254
Web-Global	VIP	Web-Services		www-hk-1: Order: 0 Weight: 1 LT: 254; www-london-1: Order: 0 Weight: 1 LT: 254; www-sf-1: Order: 0 Weight: 1 LT: 254

Rows per page: 20

3. Click the **Create Answer Group** icon. The Creating New Answer Group details page appears (Figure 6-15).

Figure 6-15 Creating New Answer Group Details Page—General Configuration


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Help | Logout
Cisco Systems
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > Answer Groups > General Configuration
Contents
General Configuration
Add Answers
Remove Answers
Submit
Cancel
148572

Creating New Answer Group

Answer Group

Name*: Web-Global

Type*: VIP

Owner*: Web-Services

Comments:

Current Members: There are no answers assigned to this answer group.

Select "Add Answers" or "Remove Answers" in the navigation bar on the left to select answers for this group.

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.

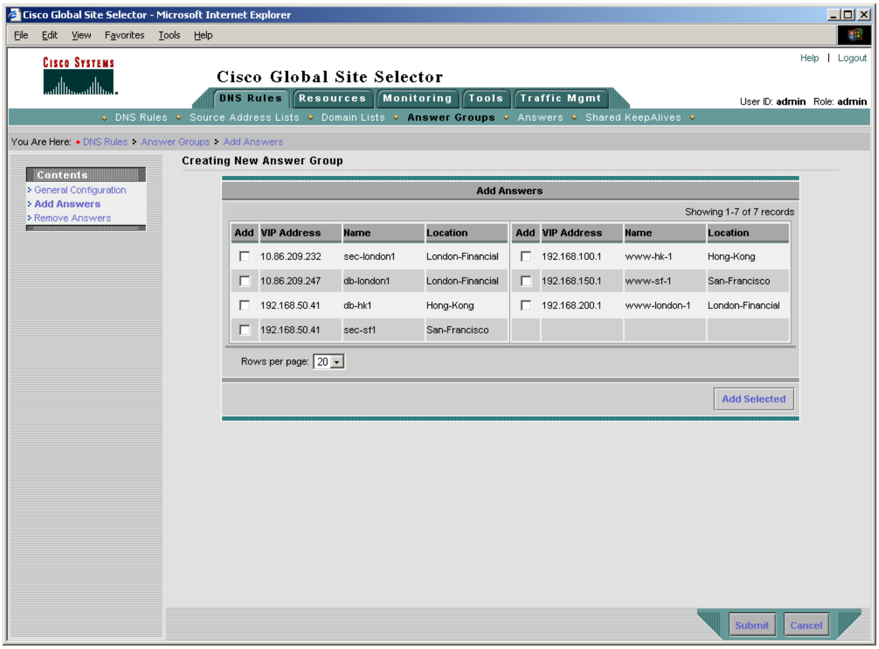
     CRA—The answer group consists of content routing agents (CRAs) for use with the boomerang server component of the GSS.

     VIP—The answer group consists of virtual IPs controlled by an SLB device such as a CSS or CSM.

5. From the Owner drop-down list, select the GSS owner with which the answer group will be associated. For details about creating an owner, refer to 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 (Figure 6-16). 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, select the answers from only the first page of answers and proceed to the next step.
    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.

Figure 6-16 Creating New Answer Group Details Page—Add Answers



Creating New Answer Group

Add Answers

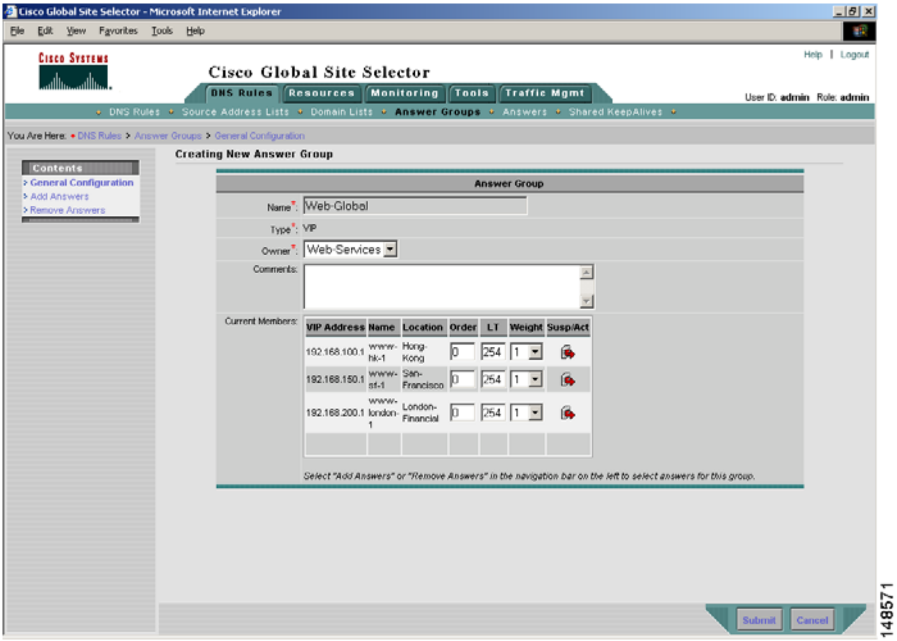
Showing 1-7 of 7 records

Add	VIP Address	Name	Location	Add	VIP Address	Name	Location
□	10.86.209.232	sec-london1	London-Financial	□	192.168.100.1	www-hk-1	Hong-Kong
□	10.86.209.247	db-london1	London-Financial	□	192.168.150.1	www-sf-1	San-Francisco
□	192.168.50.41	db-hk1	Hong-Kong	□	192.168.200.1	www-london-1	London-Financial
□	192.168.50.41	sec-sf1	San-Francisco				

Rows per page: 20

8. Click the **General Configuration** navigation link to return to the General Configuration section. The newly added answers appear in the Current Members section (Figure 6-17). There are different configuration options depending on the type of answer group.

Figure 6-17 Creating New Answer Group Details Page—Current Members



Creating New Answer Group

Answer Group

Name*: Web-Global

Type*: VIP

Owner*: Web-Services

Comments:

Current Members:

VIP Address	Name	Location	Order	LT	Weight	Susp/Act
192.168.100.1	www-hk-1	Hong-Kong	0	254	1	
192.168.150.1	www-sf-1	San-Francisco	0	254	1	
192.168.200.1	www-london-1	London-Financial	0	254	1	

Select "Add Answers" or "Remove Answers" in the navigation bar on the left to select answers for this 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.
- 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, refer to 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.

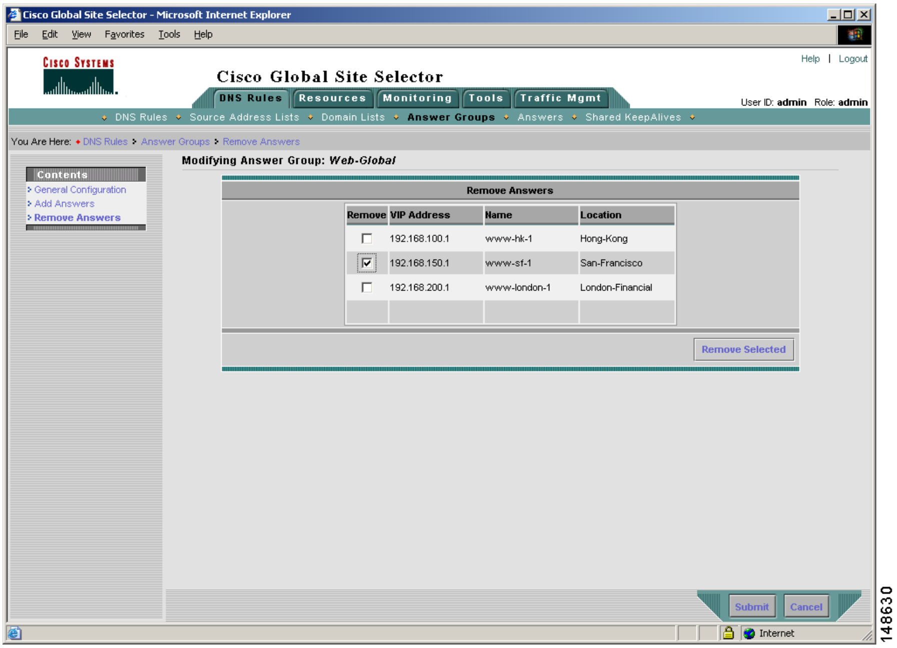
Modifying an Answer Group

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:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears (see Figure 6-14).
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 wish to add to the answer group. If the list of answers on your GSS network spans more than one page, select the answers from only the first page of answers, 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 (Figure 6-18). Click the check box accompanying each answer that you wish to remove from the list, then click the **Remove Selected** button. The GSS removes the selected answers from the page.

Figure 6-18 Modifying Answer Group—Remove Answers



Modifying Answer Group: *Web-Global*

Remove Answers

Remove	VIP Address	Name	Location
☐	192.168.100.1	www-hk-1	Hong-Kong
☑	192.168.150.1	www-sf-1	San-Francisco
☐	192.168.200.1	www-london-1	London-Financial

7. Review your updated answer group under the Current Members section of the General Configuration details page (see Figure 6-17).

8. Click the **Submit** button to save your changes and return to the Answer Groups Lists page.

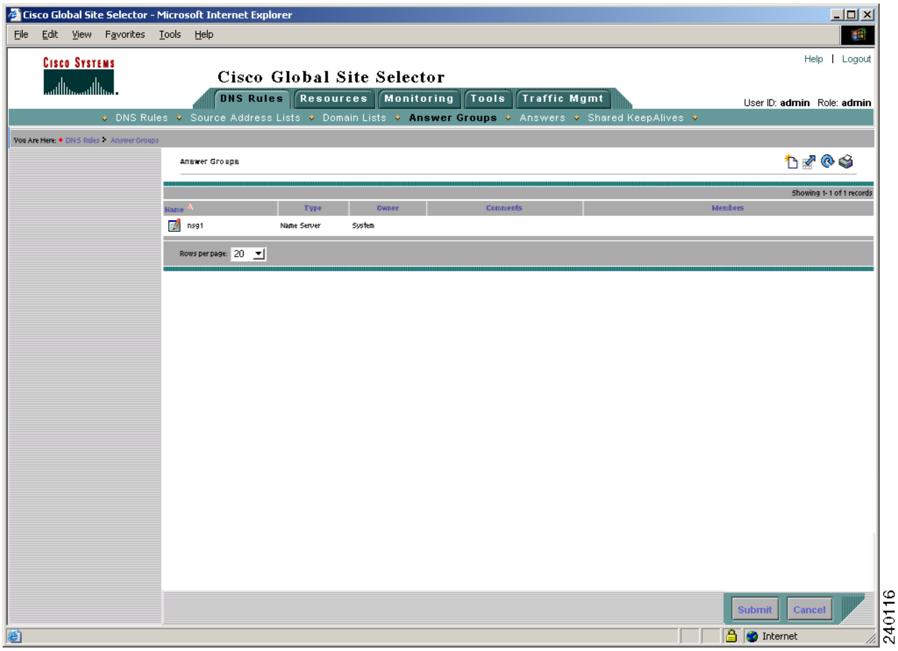
Configuring an Authority Domain for an Answer Group

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 specifying the IP address of the authority name server for the domain and the domains hosted on the name server.

To do so:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears (see Figure 6-14).
3. Click the **Create Answer Group** button and create a new answer group named NSG1 of type Name Server (see Figure 6-19).

Figure 6-19 Configuring an Authority Domain


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answer Groups
Submit
Cancel
Internet
240116

Answer Groups

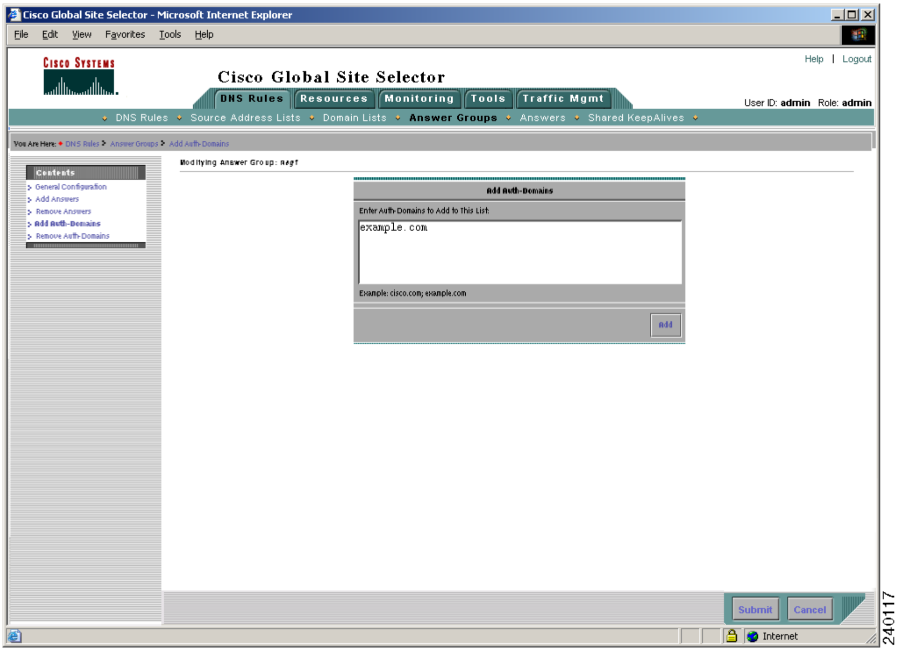
Showing 1- 1 of 1 records

Name	Type	Owner	Comments	Members
nsg1	Name Server	System		

Rows per page: 20

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. Select the **Add Auth-Domains** navigation link.
7. Enter example.com and then click **Add** to add your new Auth-Domain to the list (see Figure 6-20).

Figure 6-20 Modifying the Answer Group



Modifying Answer Group: Ragf

Add Auth-Domains

Enter Auth-Domains to Add to This List:

```
example.com
```

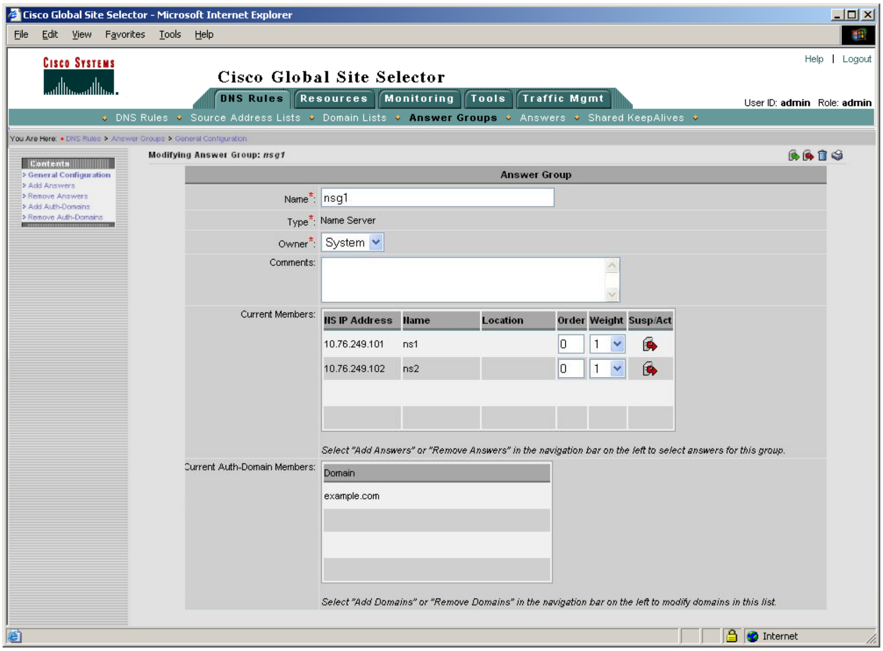
Example: cisco.com; example.com

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 (see Figure 6-21).

Figure 6-21 Displaying the Updated Answer Group



Modifying Answer Group: *nsg1*

Answer Group

Name*:	nsg1
Type*:	Name Server
Owner*:	System
Comments:	

Current Members:

NS IP Address	Name	Location	Order	Weight	Susp/Act
10.76.249.101	ns1		0	1	
10.76.249.102	ns2		0	1	

Select "Add Answers" or "Remove Answers" in the navigation bar on the left to select answers for this group.

Current Auth-Domain Members:

Domain
example.com

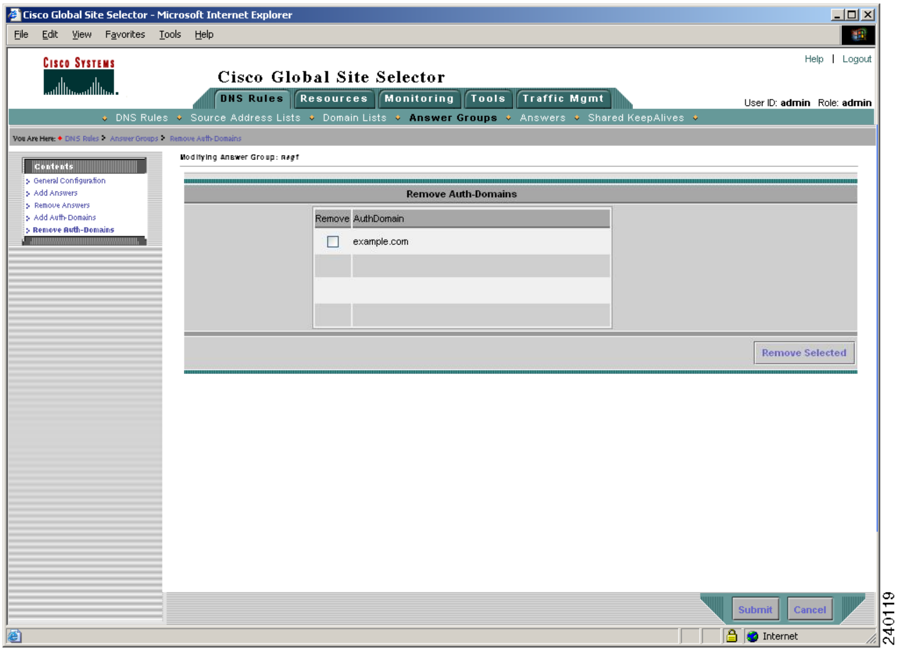
Select "Add Domains" or "Remove Domains" in the navigation bar on the left to modify domains in this list.

Deleting an Authority Domain for an Answer Group

To delete an authority domain for an answer group:

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 (see Figure 6-20).
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 the **Remove Selected** button (see Figure 6-22)

Figure 6-22 Removing an Authority Domain



Modifying Answer Group: nagf

Remove Auth-Domains

Remove	AuthDomain
□	example.com

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

To temporarily stop the GSS from directing requests to it, use 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.

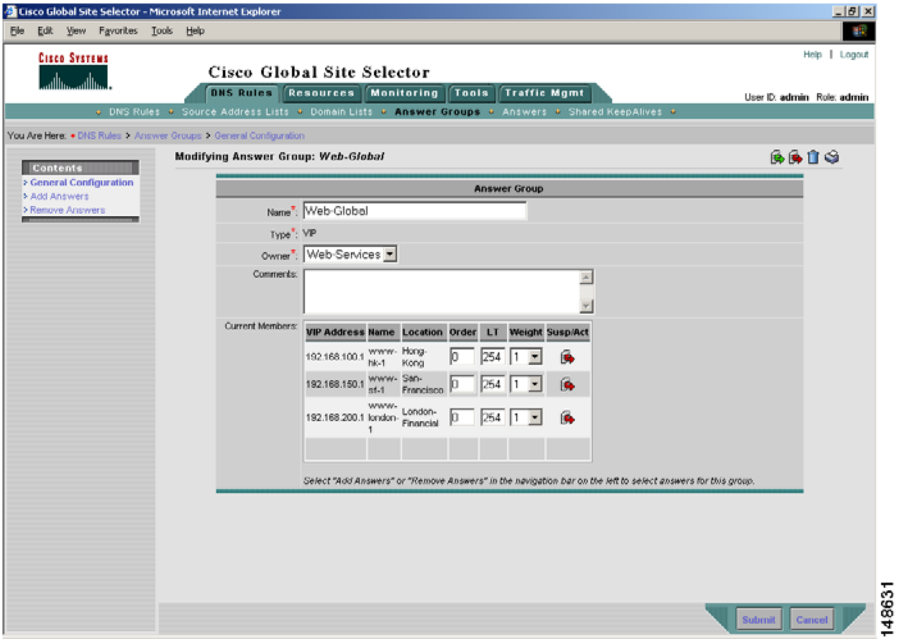
Use the Activate Answers icon to reactivate the answers in the answer group.

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:

1. From the primary GSSM GUI, click the **DNS Rules** tab.
2. Click the **Answer Groups** navigation link. The Answer Groups list page appears (see Figure 6-14).
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 (Figure 6-23).

Figure 6-23 Modifying Answer Group—Suspend Answers Icon



Modifying Answer Group: *Web-Global*

Answer Group

Name*: Web-Global

Type*: VIP

Owner*: Web-Services

Comments:

Current Members:

VIP Address	Name	Location	Order	LT	Weight	Susp/Act
192.168.100.1	www-hk-1	Hong-Kong	0	254	1	
192.168.150.1	www-sf-1	San-Francisco	0	254	1	
192.168.200.1	www-london-1	London-Financial	0	254	1	

Select "Add Answers" or "Remove Answers" in the navigation bar on the left to select answers for this group.

4. To suspend answers in the answer group, perform one of the following:
   - 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. To reactivate suspended answers in the answer group, perform one of the following:
   - 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.
7. To view the status of the suspended or activated answers, refer to Chapter 10, Monitoring GSS Global Server Load-Balancing Operation.

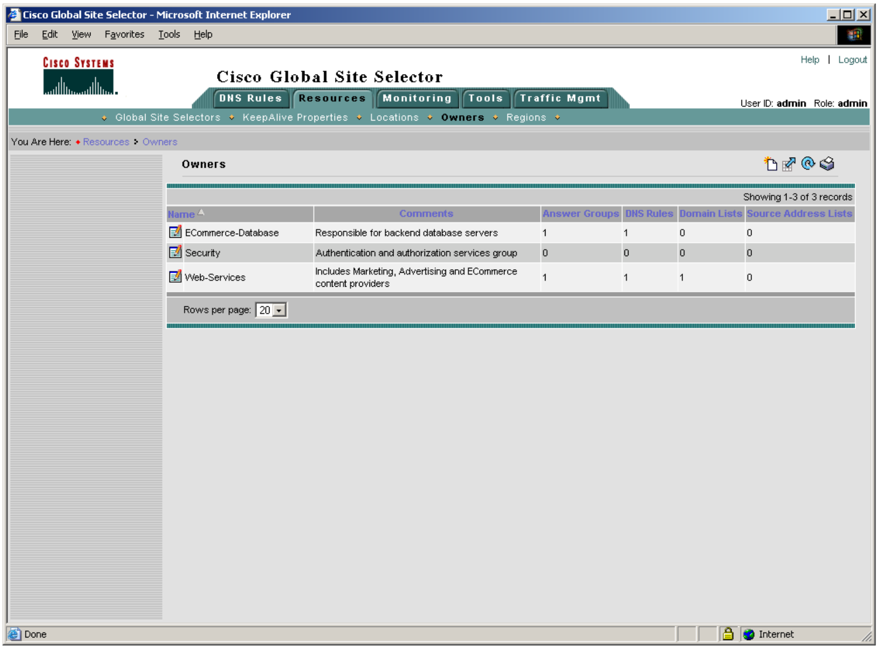
Suspending or Reactivating All Answers in an Answer Group Associated with an Owner

Answers added to answer groups can be grouped and managed according to 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:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Owners** navigation link. The Owners list page appears (Figure 6-24).

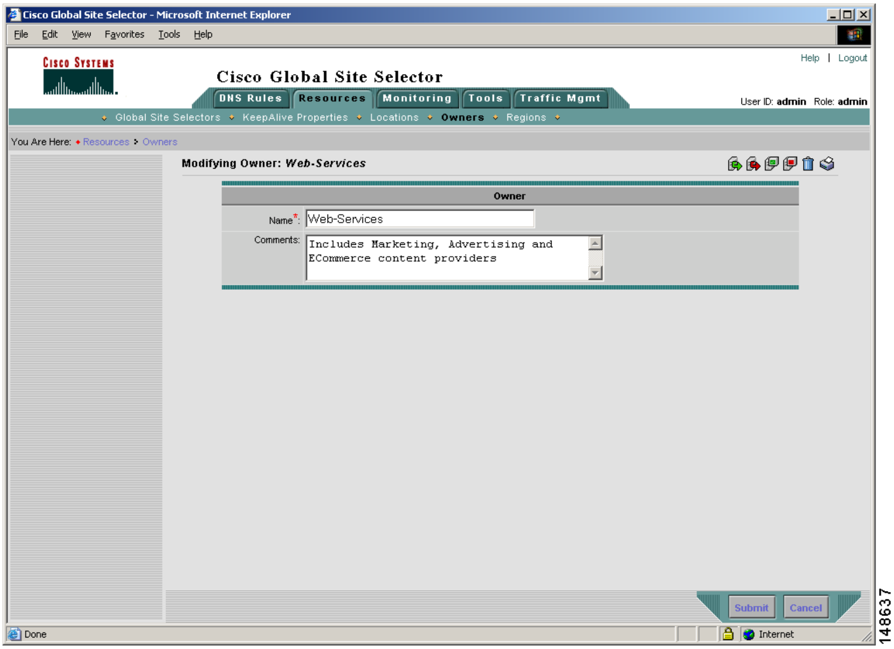
Figure 6-24 Owners List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors KeepAlive Properties Locations Owners Regions
You Are Here: Resources > Owners
Owners
Showing 1-3 of 3 records
Rows per page: 20
Done
Internet
148643

Name	Comments	Answer Groups	DNS Rules	Domain Lists	Source Address Lists
ECommerce-Database	Responsible for backend database servers	1	1	0	0
Security	Authentication and authorization services group	0	0	0	0
Web-Services	Includes Marketing, Advertising and ECommerce content providers	1	1	1	0

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 (Figure 6-25).

Figure 6-25 Modifying Owners Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources Owners
Submit
Cancel
Done
Internet
148637

Modifying Owner: *Web-Services*

Owner

Name*: Web-Services

Comments: Includes Marketing, Advertising and ECommerce content providers

4. Perform one of the following:
   - 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

To delete an answer group from the GSS, use 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. Refer to 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. Refer to the *Global Site Selector Administration Guide* for details.

To delete an answer group:

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 (see Figure 6-23).
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 constructing 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 DNS rules on your GSS network. After you configure your source address lists, domain lists, answers, and answer groups, you are ready to begin constructing the DNS rules that will control global server load balancing on your GSS network.

When building DNS rules, you specify the actions for the GSS to perform when it receives a request from a known source (a member of a source address list) for a known hosted domain (a member of a domain list). The DNS rule specifies which response (answer) is given to the requesting user's local DNS host (D-proxy) and how that answer is chosen. The GSS uses one of a variety of balance methods to determine the best response to the request, which is based on the status and load of your GSS host devices.

Note Before you create DNS rules, review the "GSS Architecture" section in Chapter 1, Introducing the Global Site Selector.

This chapter contains the following major sections:

- DNS Rule Configuration Overview
- Building DNS Rules Using the Wizard
- Building DNS Rules Using the DNS Rule Builder
- Modifying DNS Rules
- 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
- Delegation 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:

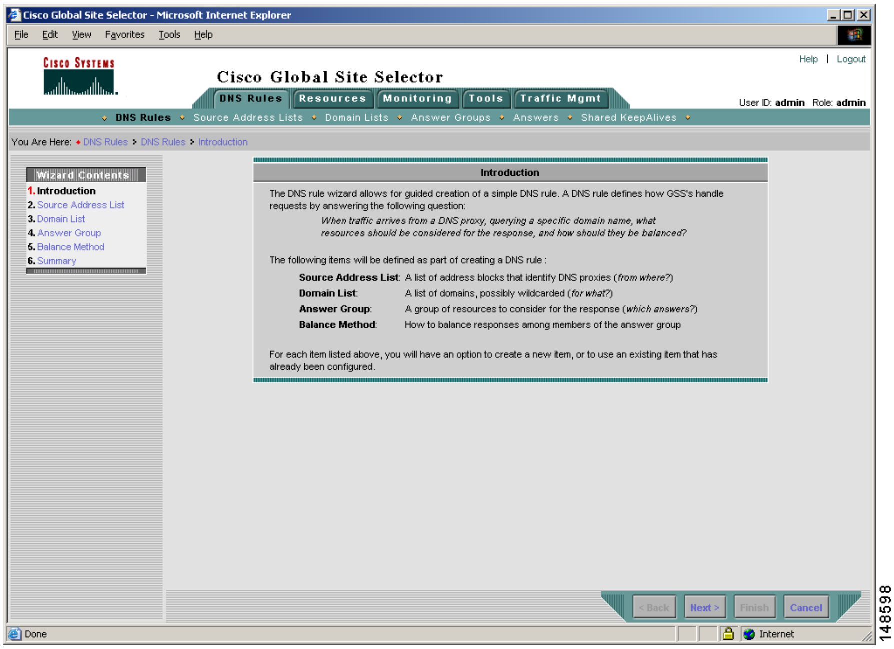
- DNS Rule Wizard
- DNS Rule Builder

DNS Rule Wizard

The DNS Rule Wizard (Figure 7-1) guides you through the process of creating a DNS rule. The DNS Rule Wizard provides explanations for each step in the rule authoring process. The DNS Rule Wizard allows you to create source address lists, domain lists, answer groups, and balance methods as required.Owners, regions, and locations, however, are not created as part of the DNS Rule Wizard and must be created prior to 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 or proximity in a DNS rule.

Figure 7-1 DNS Rule Wizard—Introduction Page



Introduction

The DNS rule wizard allows for guided creation of a simple DNS rule. A DNS rule defines how GSS's handle requests by answering the following question:

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

The following items will be defined as part of creating a DNS rule :

Source Address List:	A list of address blocks that identify DNS proxies (*from where?*)
Domain List:	A list of domains, possibly wildcarded (*for what?*)
Answer Group:	A group of resources to consider for the response (*which answers?*)
Balance Method:	How to balance responses among members of the answer group

For each item listed above, you will have an option to create a new item, or to use an existing item that has already been configured.

When you use the wizard, the **Next** and **Back** buttons step 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:

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

See the "Building DNS Rules Using the Wizard"section for details.

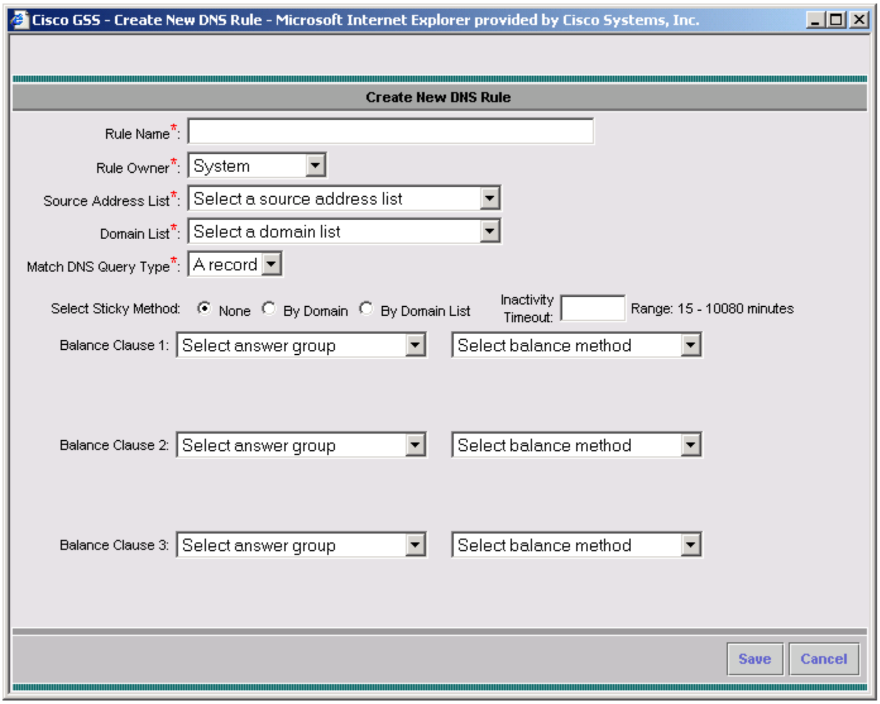
DNS Rule Builder

For experienced GSS users, use the DNS Rule Builder (Figure 7-2) to quickly assemble DNS rules from source address lists, domain lists, owners, and answers that you have already created. Using the fields and drop-down menus provided, 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, with parameters established to determine when a clause is skipped and the next clause used. A balance clause is skipped when any one of the following conditions exits:

- A least-loaded balance method is selected and the load threshold for all online answers is exceeded.
- The VIP answers in the specified VIP answer group are offline.
- Proximity is enabled for a VIP-type answer group and the DRP agents do not return any RTT values that meet the value set for **acceptable-rtt**.
- All answers in a CRA- or NS-type answer group are offline and keepalives are enabled to monitor the answers.

Figure 7-2 DNS Rule Builder Window



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Create New DNS Rule

Rule Name*:

Rule Owner*: System

Source Address List*: Select a source address list

Domain List*: Select a domain list

Match DNS Query Type*: A record

Select Sticky Method: ● None ○ By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes

Balance Clause 1: Select answer group Select balance method

Balance Clause 2: Select answer group Select balance method

Balance Clause 3: Select answer group Select balance method

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 in the event that the first answer group and balance method specified does not yield an answer.

To access the DNS Rule Builder:

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

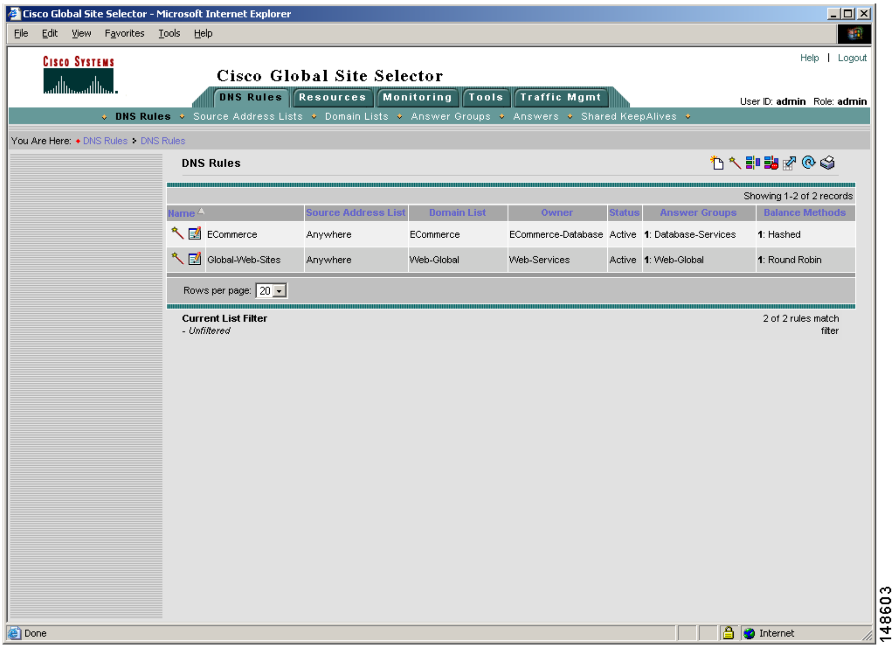
To create a DNS rule using the DNS Rule Wizard:

Note Owners, regions, and locations are not created as part of the DNS Rule Wizard and must be created before you use the wizard.

Note 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 or proximity in a DNS rule.

1. From the primary GSSM GUI, click the **DNS Rules** tab, then the **DNS Rules** navigation link. The DNS Rules list appears (Figure 7-3).

Figure 7-3 DNS Rules List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > DNS Rules
Done
Internet
148603

DNS Rules

Showing 1-2 of 2 records

Name	Source Address List	Domain List	Owner	Status	Answer Groups	Balance Methods
ECommerce	Anywhere	ECommerce	ECommerce-Database	Active	1: Database-Services	1: Hashed
Global-Web-Sites	Anywhere	Web-Global	Web-Services	Active	1: Web-Global	1: Round Robin

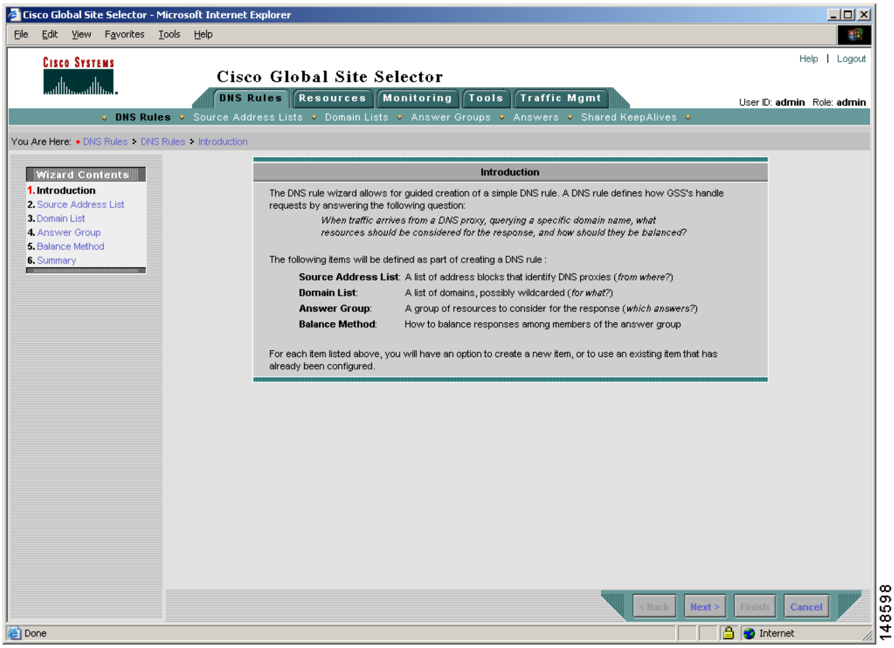
Rows per page: 20

Current List Filter
- *Unfiltered*

2 of 2 rules match filter

2. Click the **Rule Wizard** icon. The DNS Rule Wizard introduction page appears (Figure 7-4). This page provides an overview of the steps necessary to create a DNS rule.

Figure 7-4 DNS Rule Wizard—Introduction Page



Introduction

The DNS rule wizard allows for guided creation of a simple DNS rule. A DNS rule defines how GSS's handle requests by answering the following question:

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

The following items will be defined as part of creating a DNS rule :

Source Address List:	A list of address blocks that identify DNS proxies (*from where?*)
Domain List:	A list of domains, possibly wildcarded (*for what?*)
Answer Group:	A group of resources to consider for the response (*which answers?*)
Balance Method:	How to balance responses among members of the answer group

For each item listed above, you will have an option to create a new item, or to use an existing item that has already been configured.

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.

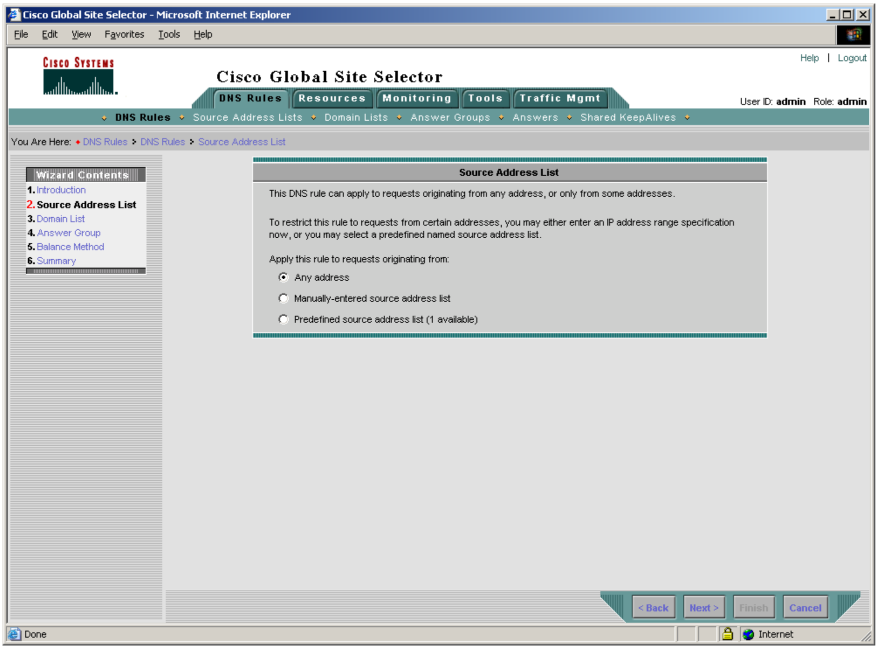
   The following procedures describe how to configure the properties for the individual pages in the DNS Rule Wizard:

   - 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
   - Selecting 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 (Figure 7-5) allows you to identify a source address list, a list of address blocks that identify DNS proxies.

Figure 7-5 DNS Rule Wizard—Source Address List Page 1



Source Address List

This DNS rule can apply to requests originating from any address, or only from some addresses.

To restrict this rule to requests from certain addresses, you may either enter an IP address range specification now, or you may select a predefined named source address list.

Apply this rule to requests originating from:

● Any address

○ Manually-entered source address list

○ Predefined source address list (1 available)

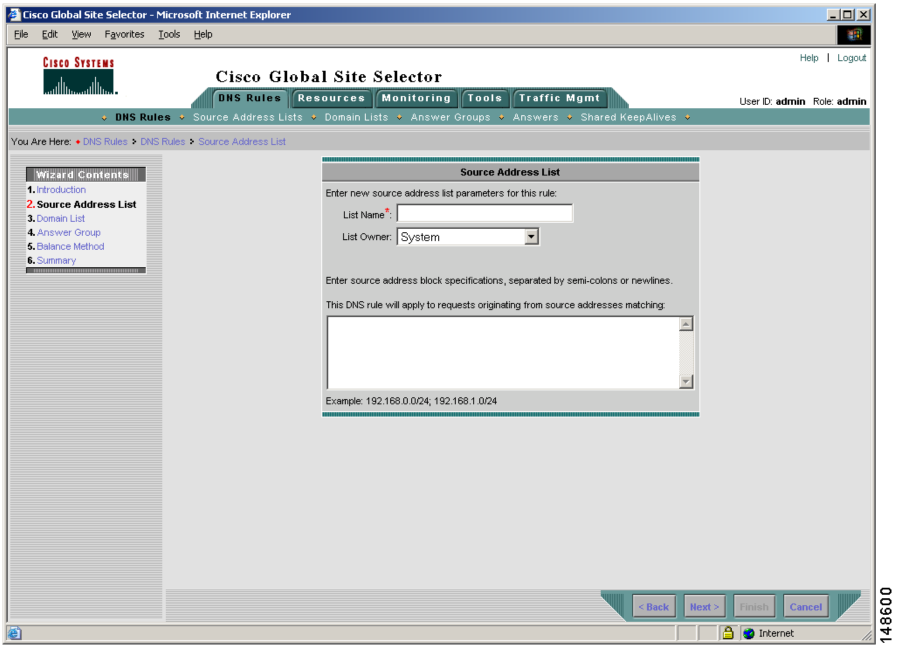
To identify a source address list in the DNS Rule Wizard:

1. Perform one of the following actions:
   - To apply the DNS rule to requests originating from any DNS proxy, click the **Any Address** option, then click **Next**. Proceed to 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 the **Manually-entered source address list** option, 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 the **Predefined source address list** option, 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 (Figure 7-6) of the wizard to create your Source Address List. After you configure your source address list using the wizard, it is available for use by other DNS rules.

Figure 7-6 DNS Rule Wizard—Source Address List Page 2


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules > Source Address List
Wizard Contents
1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary
< Back
Next >
Finish
Cancel
Internet
148600

Source Address List

Enter new source address list parameters for this rule:

List Name*:

List Owner: System

Enter source address block specifications, separated by semi-colons or newlines.

This DNS rule will apply to requests originating from source addresses matching:

Example: 192.168.0.0/24; 192.168.1.0/24

a. Enter a name for your Source Address List in the List Name field.

b. Optionally, click the List Owner drop-down list and select a GSS owner name.

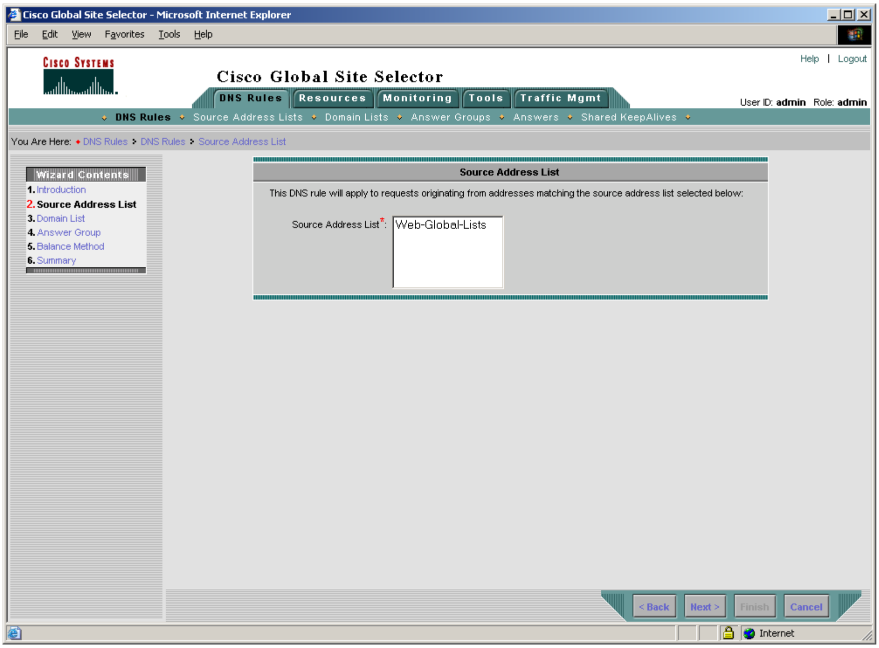
c. In the space provided, enter one or more source classless interdomain routing (CIDR)-format IP addresses that make up the list. You can enter individual IP addresses or address blocks. If you want to enter multiple IP addresses, separate the addresses using semicolons.

For example:192.168.1.110/32; 192.168.10.0/24; 192.161.0.0/16

d. 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 (Figure 7-7) of the wizard to select an existing source address list.

Figure 7-7 DNS Rule Wizard—Source Address List Page 3


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules > Source Address List
Wizard Contents
1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary
< Back
Next >
Finish
Cancel
Internet
148601

Source Address List

This DNS rule will apply to requests originating from addresses matching the source address list selected below:

Source Address List*: Web-Global-Lists

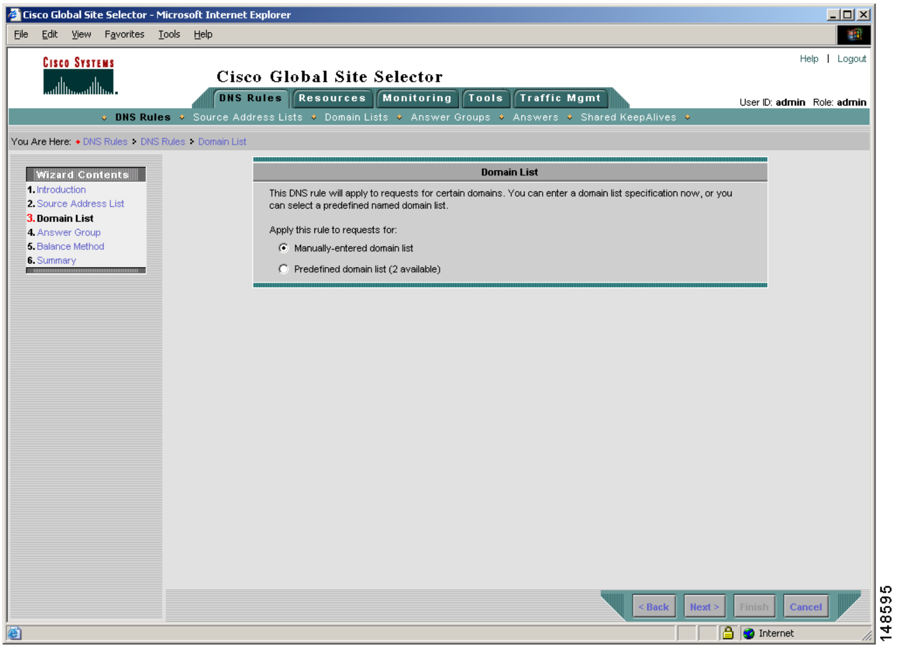
a. Click the name of the source address list in the list to highlight it.

b. 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 (Figure 7-8) 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).

Figure 7-8 DNS Rule Wizard—Domain List Page 1



Domain List

This DNS rule will apply to requests for certain domains. You can enter a domain list specification now, or you can select a predefined named domain list.

Apply this rule to requests for:

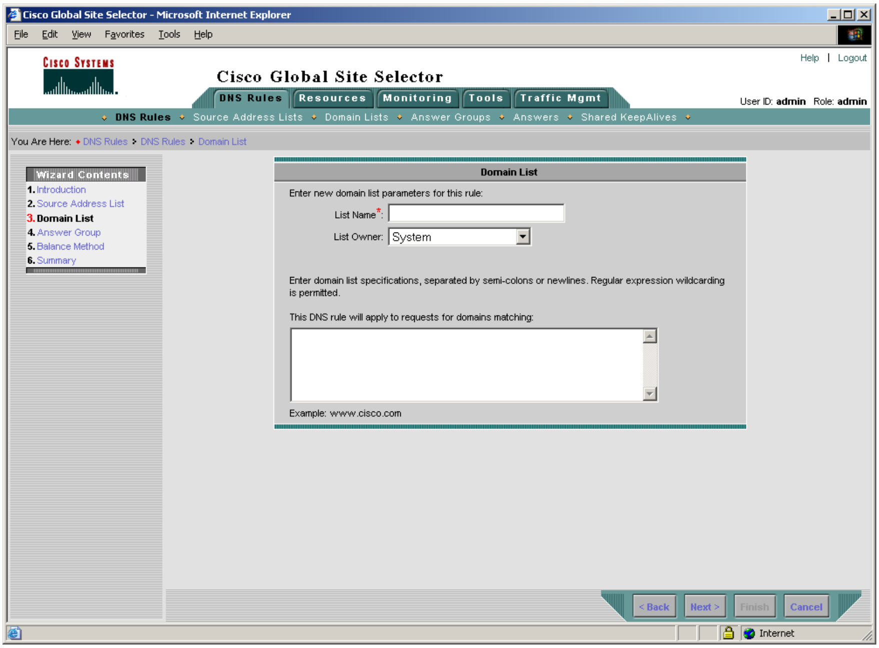
● Manually-entered domain list

○ Predefined domain list (2 available)

To specify a domain list in the DNS Rule Wizard:

1. Perform one of the following:
   - To apply the DNS rule to requests for a hosted domain that you want to configure, click the **Manually-entered domain list** option, then click **Next**. Proceed to step 2 for information on using the Domain List Page 2 in the wizard.
   - To apply the DNS Rule to requests for a domain from a list of hosted domains previously configured using the Domain Lists function, click the **Predefined domain list** option, then click **Next**. Proceed to step 3 for information on using the Domain List Page 3 in the wizard.
2. If you chose the Manually-entered Domain List option in the Domain List section of the wizard, use the Domain List Page 2 (Figure 7-9) of the wizard to manually configure the requested domains names. After you configure your domain list using the DNS Rule Wizard, it is available for use by other DNS rules.

Figure 7-9 DNS Rule Wizard—Domain List Page 2



Domain List

Enter new domain list parameters for this rule:

List Name*:

List Owner: System

Enter domain list specifications, separated by semi-colons or newlines. Regular expression wildcarding is permitted.

This DNS rule will apply to requests for domains matching:

Example: www.cisco.com

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

b. Optionally, click the List Owner drop-down list and select 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 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, for example:

```
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:

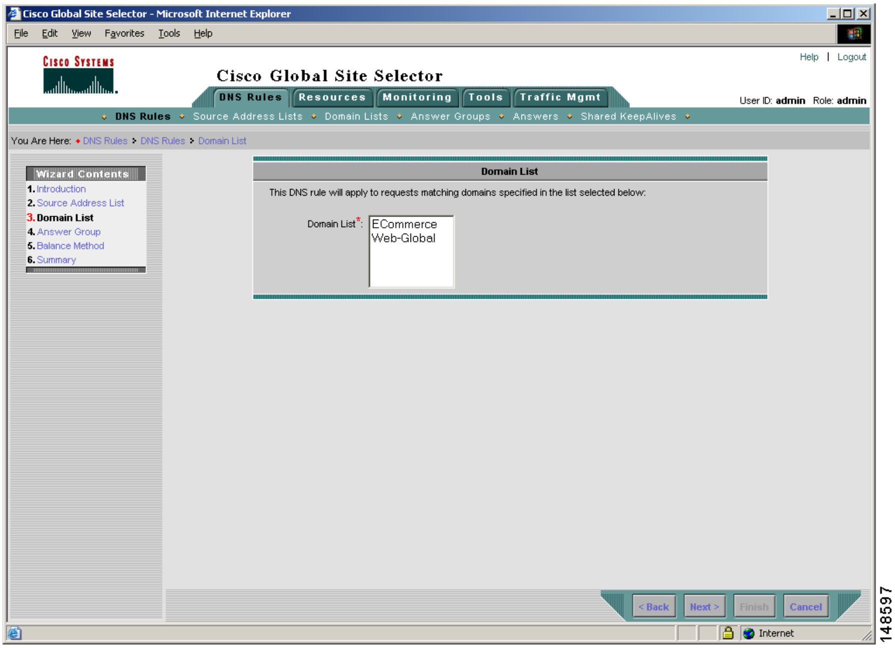
```
.*\.cisco\.com
```

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

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.

3. If you chose the Predefined Domain List option, use Domain List Page 3 (Figure 7-10) of the wizard to select from a list of previously configured domains.

Figure 7-10 DNS Rule Wizard—Domain List Page 3



Domain List

This DNS rule will apply to requests matching domains specified in the list selected below:

Domain List*: ECommerce
Web-Global

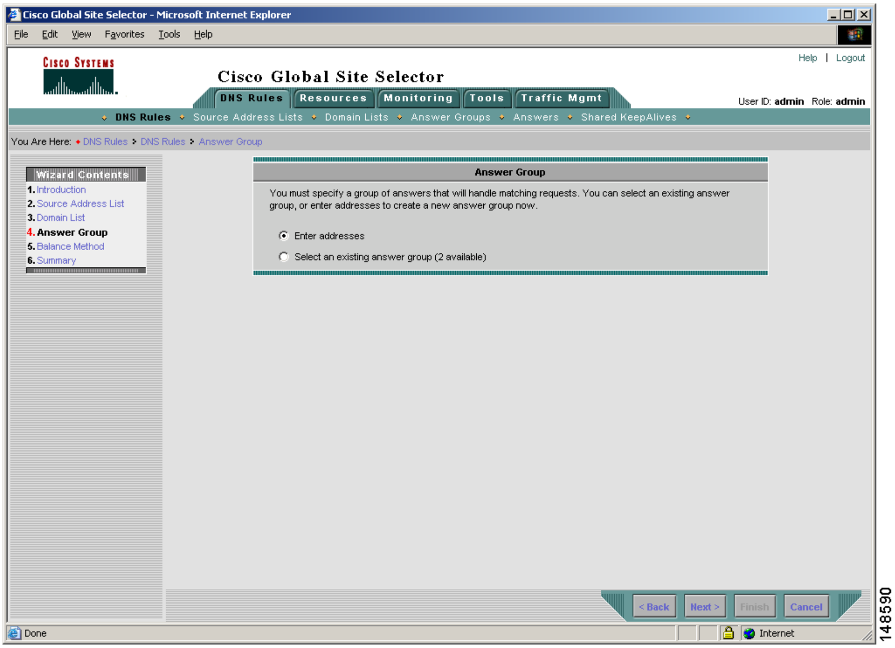
a. Click the name of the domain list so that its name is highlighted.

b. Click **Next** to select 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 (Figure 7-11) 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.

Figure 7-11 DNS Rule Wizard—Answer Group Page 1


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules > Answer Group
Wizard Contents
1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary
< Back
Next >
Finish
Cancel
Done
Internet
148590

Answer Group

You must specify a group of answers that will handle matching requests. You can select an existing answer group, or enter addresses to create a new answer group now.

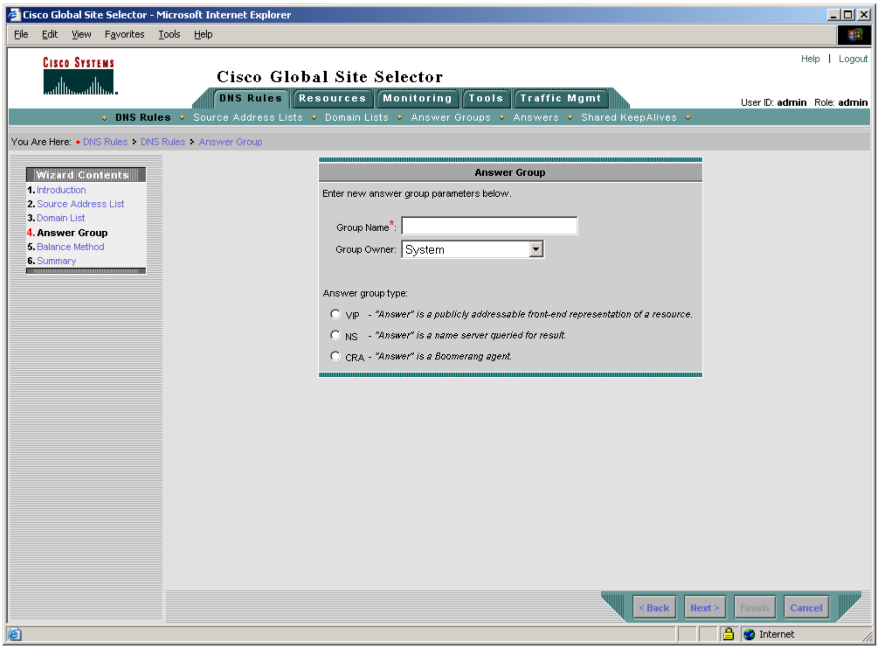
● Enter addresses

○ Select an existing answer group (2 available)

To configure an answer group in the DNS Rule Wizard:

1. Perform one of the following:
   - To have the DNS rule respond to the request for the hosted domain using resources (answers) that you want to configure, click the **Enter addresses** option, then click **Next**. Proceed to step 2 for information on using the Answer Group Page 2 in the wizard.
   - To have the DNS rule respond to the request for the hosted domain using resources (answers) previously configured using the Answer Group function, click the **Select an existing answer group** option, then click **Next**. Proceed to step 3 for information on using the Answer Group Page 3 in the wizard.
2. If you chose the Enter Addresses option in the Answer Group section of the wizard, use Answer Group Page 2 (Figure 7-12) in the wizard to create your answer group. After you configure your answer group using the DNS Rule Wizard, it is available for use by other DNS rules.

Figure 7-12 DNS Rule Wizard—Answer Group Page 2



Answer Group

Enter new answer group parameters below.

Group Name*:

Group Owner: System

Answer group type:

○ VIP - *"Answer" is a publicly addressable front-end representation of a resource.*

○ NS - *"Answer" is a name server queried for result.*

○ CRA - *"Answer" is a Boomerang agent.*

a. Enter a name for your answer group in the Group Name field.

b. Optionally, select 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.

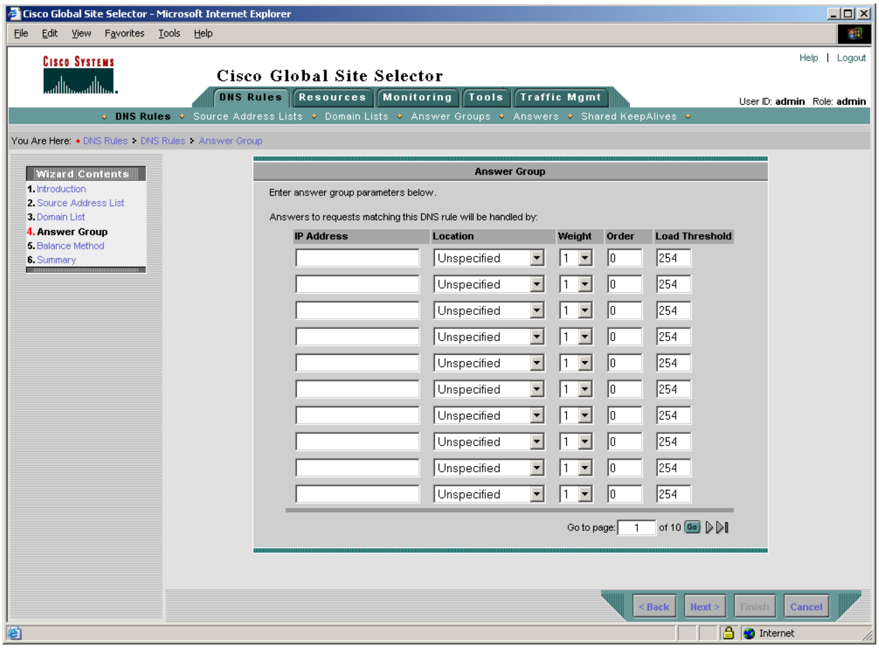
   Name Server—A configured DNS name server on your network that can answer queries that the GSS cannot resolve.

   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 3.

3. Use Answer Group Page 3 of the DNS Rule Wizard (Figure 7-13) to configure answers for the specified answer group type: VIP, NS, or CRA.

Figure 7-13 DNS Rule Wizard—Answer Group Page 3



Wizard Contents

1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary

Answer Group

Enter answer group parameters below.

Answers to requests matching this DNS rule will be handled by:

IP Address	Location	Weight	Order	Load Threshold
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254
	Unspecified	1	0	254

Go to page: 1 of 10 Go

4. 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 select 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 that preceding VIPs on the list are unavailable. The GSS supports gaps in numbering in an ordered list.

Note For answers that have the same order number in an answer group, the GSS 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 unavailable to handle further requests.

- If configuring a new name server-type answer group, perform the following steps to identify the name servers providing the answers for the 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 select 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 gaps in numbering in an ordered list.

Note For answers that have the same order number in an answer group, the GSS will only use the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

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

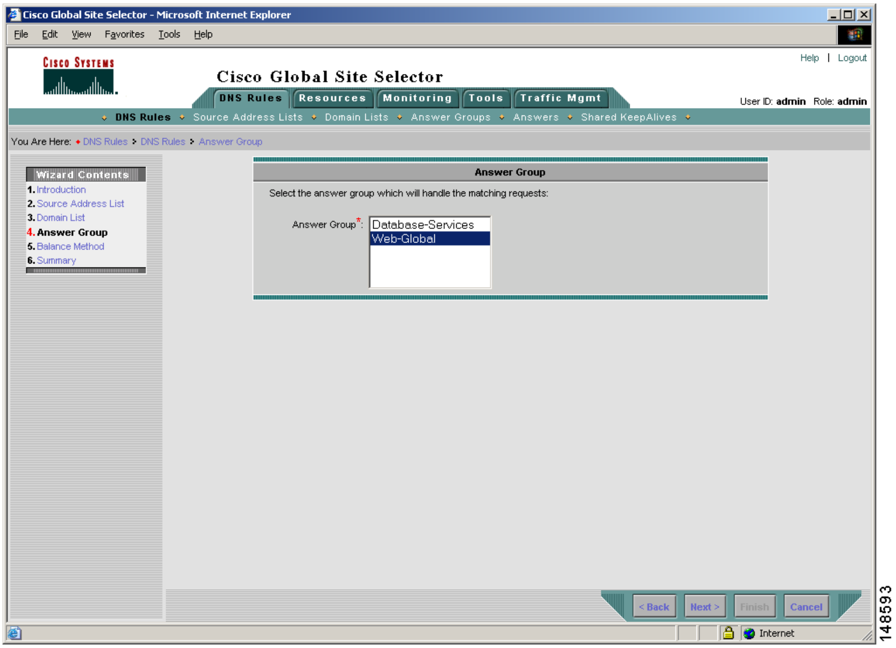
a. Enter the address of each CRA that belongs to the answer group in the IP Address fields provided.

b. For each CRA IP address, select 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 Selecting a Balance Method in the DNS Rule Wizard section for information.

5. If you chose the Select an Existing Answer Group option, use Answer Group Page 4 (Figure 7-14) in the wizard to select from a series of previously configured answers.

Figure 7-14 DNS Rule Wizard—Answer Group Page 4


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules > Answer Group
Wizard Contents
1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary
< Back
Next >
Finish
Cancel
Internet
148593

Answer Group

Select the answer group which will handle the matching requests:

Answer Group*: Database-Services, Web-Global (selected)

a. Click the name of the answer group in the list so that the name is highlighted.

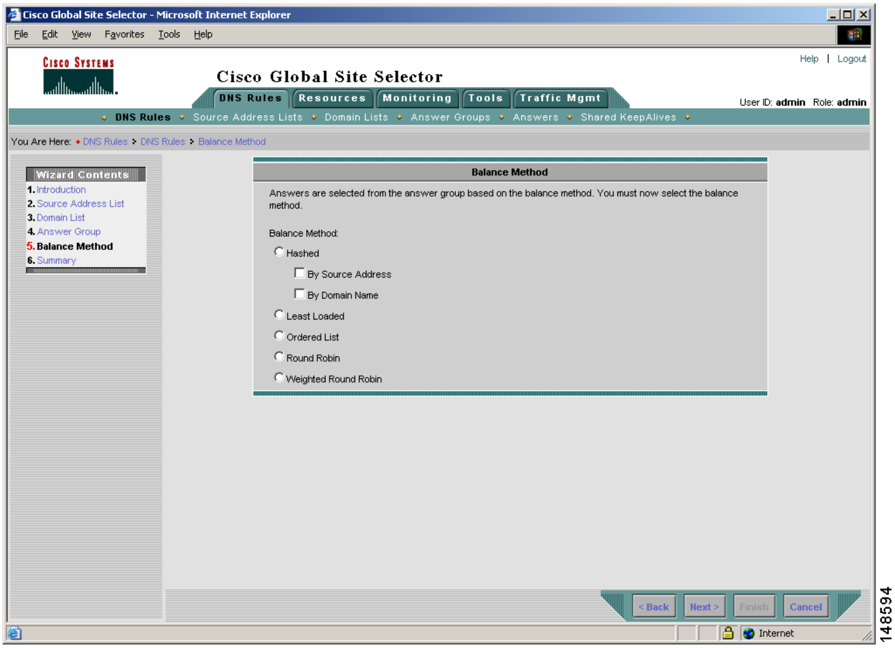
b. Click **Next** to select the answer group and proceed to the Balance Method details page of the DNS Rule Wizard. See the Selecting a Balance Method in the DNS Rule Wizard section for information.

Selecting a Balance Method in the DNS Rule Wizard

The Balance Method page of the DNS Rule Wizard (Figure 7-15) allows you to select a balance method that specifies how a GSS answer should be selected 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 select.

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).

Figure 7-15 DNS Rule Wizard—Balance Method Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules > Balance Method
Wizard Contents
1. Introduction
2. Source Address List
3. Domain List
4. Answer Group
5. Balance Method
6. Summary
< Back
Next >
Finish
Cancel
Internet
148594

Balance Method

Answers are selected from the answer group based on the balance method. You must now select the balance method.

Balance Method:

○ Hashed
□ By Source Address
□ By Domain Name
○ Least Loaded
○ Ordered List
○ Round Robin
○ Weighted Round Robin

To select a balance method in the DNS Rule Wizard:

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 gaps in numbering in an ordered list.

   Note For answers that have the same order number in an answer group, the GSS will only use the first answer that contains the number. We recommend that you specify a unique order number for each answer in an answer group.

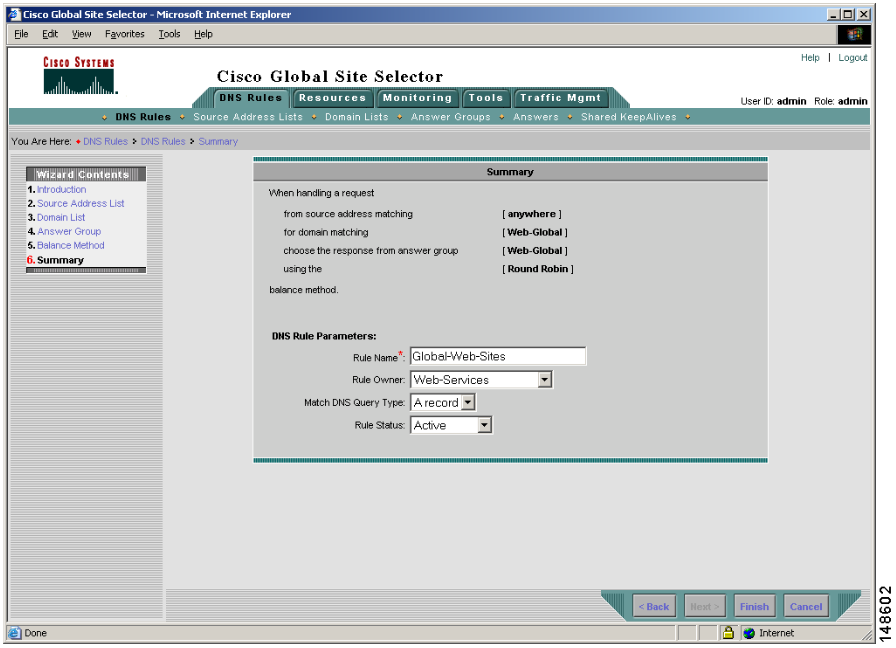
   - **Round Robin**—The GSS cycles through the list of answers that are available as requests are received.
   - **Weighted Round Robin**—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value 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 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 (Figure 7-16) allows you to verify information about your DNS rule, including information on the selected source address list, domain list, answer group, and balance method.

Figure 7-16 DNS Rule Wizard—Summary Page



Summary

When handling a request

from source address matching	[**anywhere**]
for domain matching	[**Web-Global**]
choose the response from answer group	[**Web-Global**]
using the	[**Round Robin**]

balance method.

DNS Rule Parameters:

Rule Name*: Global-Web-Sites

Rule Owner: Web-Services

Match DNS Query Type: A record

Rule Status: Active

To complete your DNS rule in the Summary page:

1. Enter a name for your DNS Rule in the **Rule Name** field.
2. Optionally, associate the rule with an GSS owner by selecting an owner name from the **Rule Owner** drop-down list.

3. Indicate the type of DNS queries that apply to this rule. Select a query type from the **Match DNS Query Type** drop-down list:

   - **All**—The DNS rule is applied to all DNS queries originating from a host on the configured source address list. For any request other than an A-record query (for example, MX or CNAME record), the GSS forwards the request to a name server configured in one of the three Balance Clauses. When the GSS receives the response from the name server, it then delivers the response to the requesting client D-proxy.

     When you select **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 then make a subsequent A-record query.

4. Select an operating status for the rule from the Rule Status 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.

5. Click **Finish** to save your DNS Rule. You return to the DNS Rules list page.

Building DNS Rules Using the DNS Rule Builder

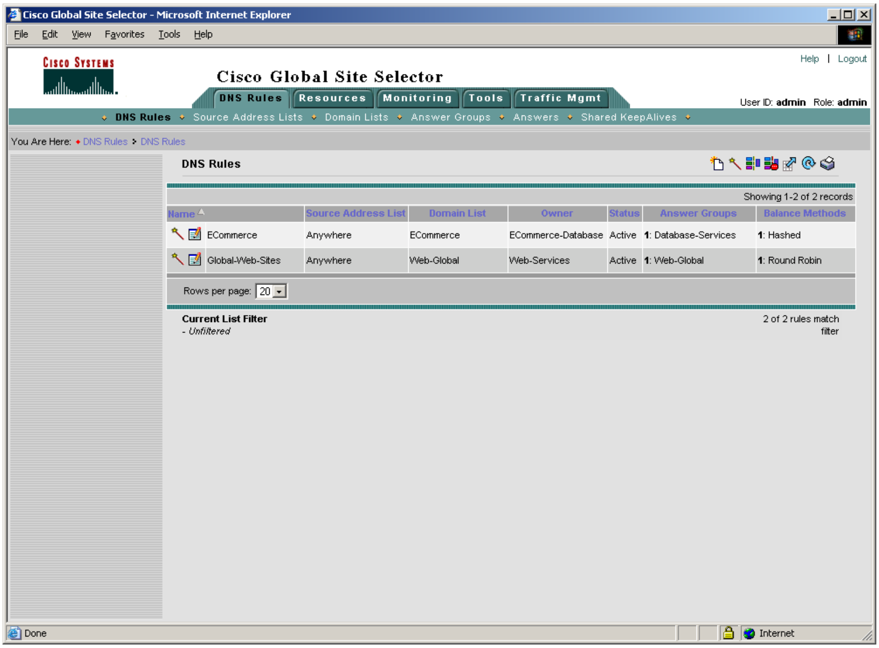
If you are comfortable with the process of building a DNS rule and have previously configured your domain lists, answers, and answer groups, use the DNS Rule Builder to quickly assemble a DNS rule.

If you intend to use the DNS rule builder for more advanced GSS load-balancing applications such as DNS sticky or network proximity, refer to Chapter 8, Configuring DNS Sticky or Chapter 9, Configuring Network Proximity for the configuration procedures.

To create a DNS rule using the DNS Rule Builder:

1. From the primary GSSM GUI, click the **DNS Rules** tab, then click the **DNS Rules** navigation link. The DNS Rules list appears (Figure 7-17).

Figure 7-17 DNS Rules List Page



DNS Rules

Showing 1-2 of 2 records

Name	Source Address List	Domain List	Owner	Status	Answer Groups	Balance Methods
ECommerce	Anywhere	ECommerce	ECommerce-Database	Active	1: Database-Services	1: Hashed
Global-Web-Sites	Anywhere	Web-Global	Web-Services	Active	1: Web-Global	1: Round Robin

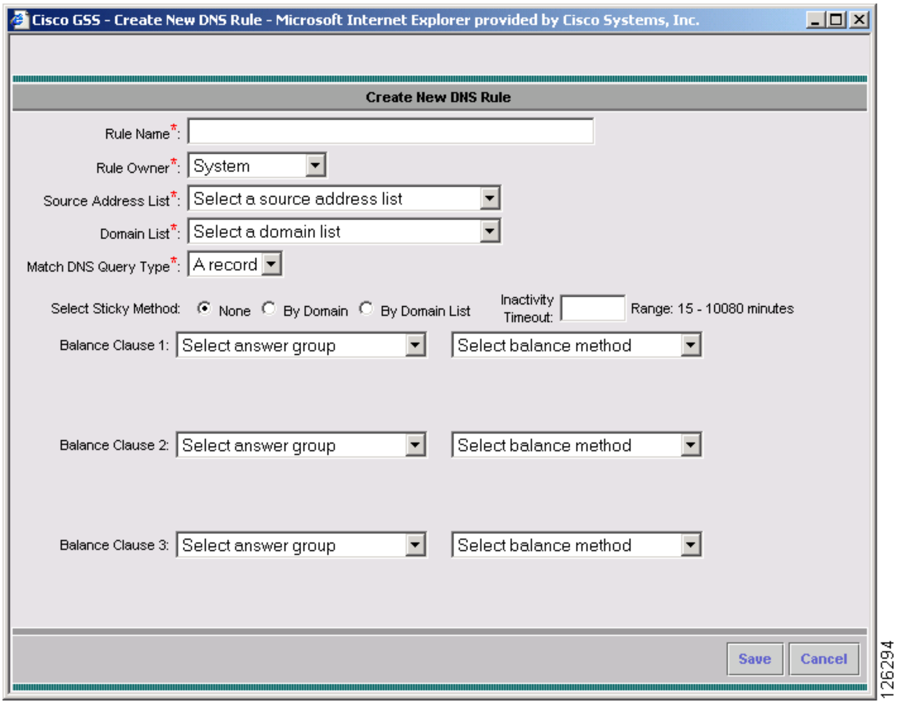
Rows per page: 20

Current List Filter
- *Unfiltered*

2 of 2 rules match filter

2. Click the **Open Rule Builder** icon. The DNS Rule Builder page opens in a separate window (Figure 7-18).

Figure 7-18 Create New DNS Rule Window



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Create New DNS Rule

Rule Name*:

Rule Owner*: System

Source Address List*: Select a source address list

Domain List*: Select a domain list

Match DNS Query Type*: A record

Select Sticky Method: ● None ○ By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes

Balance Clause 1: Select answer group Select balance method

Balance Clause 2: Select answer group Select balance method

Balance Clause 3: Select answer group Select balance method

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 drop-down list, indicate what type of DNS queries applies to this rule:

   - **All**—The DNS rule is applied to all DNS queries originating from a host on the configured source address list. For any request other than an A-record query (for example, MX or CNAME record), the GSS forwards the request to a name server configured in one of the three Balance Clauses. When the GSS receives the response from the name server, it then delivers the response to the requesting client D-proxy.

     When you select **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 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 query.

8. To disable sticky for the DNS rule, leave the Select Sticky Method option set to **None** (default). This setting overrides the enabled state on the Global Sticky Configuration details page.

   If you plan to configure DNS sticky in the DNS rule, refer to "Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups" in Chapter 8, Configuring DNS Sticky.

9. At the Balance Clause 1 heading:
   - Select 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.
   - Select 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) 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.

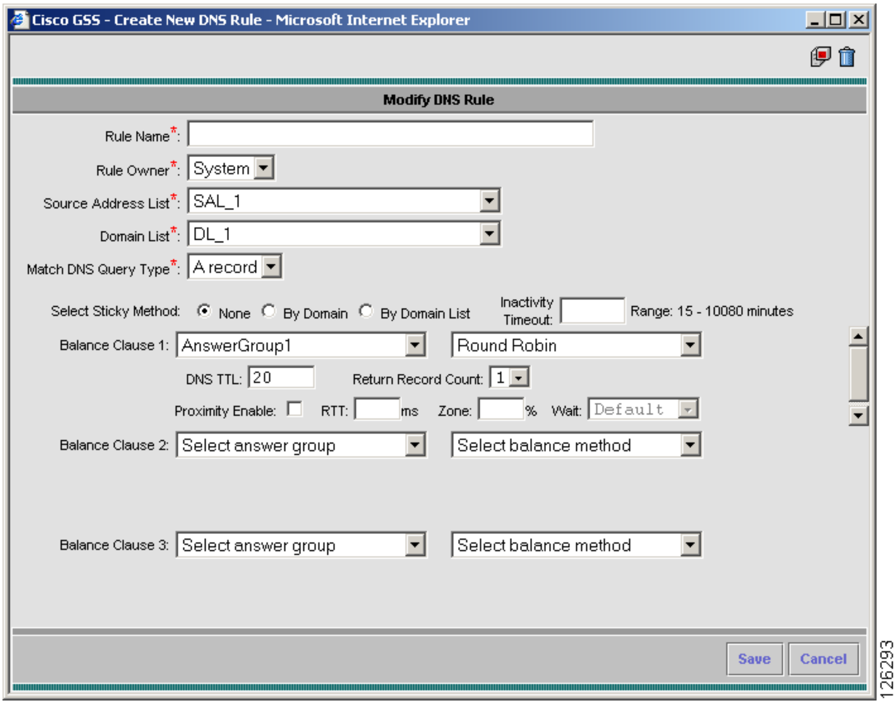
  By Source Address—The GSS selects the answer based on a hash value created from the source address of the request.

  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. Least Loaded 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 gaps in numbering 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.

11. 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. Figure 7-19 shows an example of the DNS Rule window with a selected VIP-type answer group.

Figure 7-19 Create New DNS Rule Window With VIP-Type Answer Group Fields



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer

Modify DNS Rule

Rule Name*:

Rule Owner*: System

Source Address List*: SAL_1

Domain List*: DL_1

Match DNS Query Type*: A record

Select Sticky Method: ● None ○ By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes

Balance Clause 1: AnswerGroup1 Round Robin

DNS TTL: 20 Return Record Count: 1

Proximity Enable: □ RTT: ms Zone: % Wait: Default

Balance Clause 2: Select answer group Select balance method

Balance Clause 3: Select answer group Select balance method

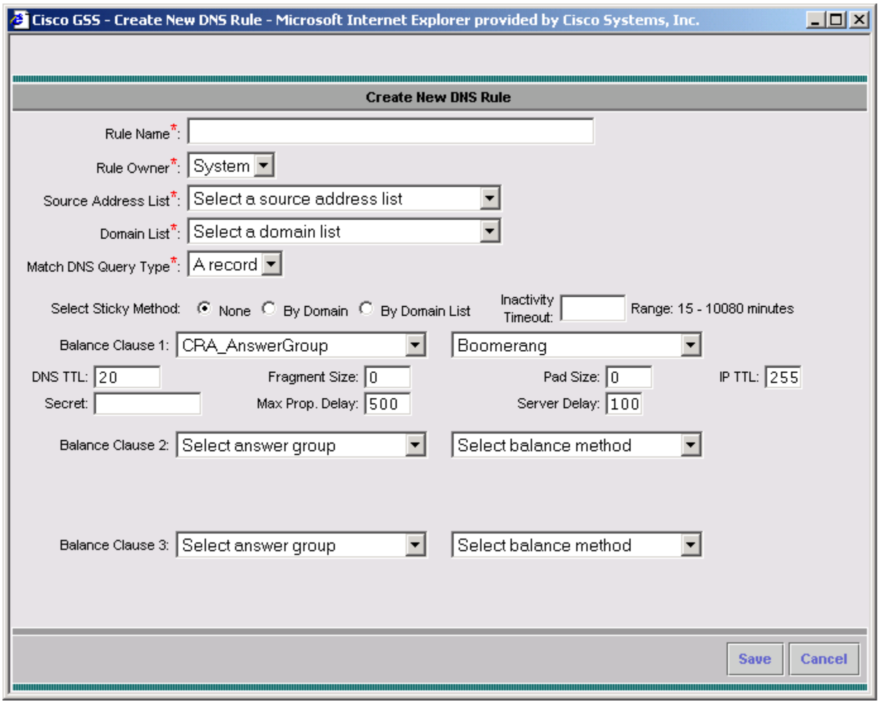
Configure the following VIP-type configuration information in the fields provided below the active balance clause:

- **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.

If you plan to configure network proximity as part of the DNS rule balance clause, refer to the "Using the DNS Rule Builder to Add Proximity to a DNS Rule" section in Chapter 9, Configuring Network Proximity.

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. Figure 7-20 shows an example of the DNS Rule Builder window with a selected CRA-type answer group.

Figure 7-20 Create New DNS Rule Window With CRA-Type Answer Group Fields



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Create New DNS Rule

Rule Name*:
Rule Owner*: System
Source Address List*: Select a source address list
Domain List*: Select a domain list
Match DNS Query Type*: A record
Select Sticky Method: ● None ○ By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes
Balance Clause 1: CRA_AnswerGroup Boomerang
DNS TTL: 20 Fragment Size: 0 Pad Size: 0 IP TTL: 255
Secret: Max Prop. Delay: 500 Server Delay: 100
Balance Clause 2: Select answer group Select balance method
Balance Clause 3: Select answer group Select balance method

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 consider 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) that is observed before the boomerang server component of the GSS forwards a DNS request to a CRA.
- **Server Delay**—The maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS returns the address of its "last gasp" server as a response to the requesting name server.

13. Repeat steps 9 through 12 to select additional answer group and balance method pairings for Balance Clause 2 and Balance Clause 3. These answer pairs only apply when the preceding clause is unable to provide an answer for the DNS query.

Note Always follow a balance clause that uses a CRA-type answer group with a balance clause that uses a VIP-type answer group. Doing so ensures that if none of the Content Routing Agenents successfully respond to the DNS race request, a "last gasp" server response from the VIP-type balance clause is sent to the requesting name server.

14. Click **Save** to save your DNS Rule. You return to the DNS Rules list page. The DNS rule is now active and processing incoming DNS requests.

Modifying DNS Rules

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

To modify a DNS rule using the DNS Rule Builder:

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:

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 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:

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. Click the **Suspend** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to suspend the DNS rule.
4. Click **OK** to confirm your decision and return to the DNS Rule list page. The status of the DNS rule appears as “Suspended”.

To suspend a DNS rule from the DNS Rule Wizard:

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 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 (see Figure 7-16).
4. From the Rule Status drop down list, select 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”.

Reactivating a DNS Rule

To reactivate operation of a suspended DNS rule from the DNS Rule Builder:

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".

To reactivate operation of a suspended DNS rule from the DNS Rule Wizard:

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 (see Figure 7-16).
4. From the Rule Status drop down list, select the **Active** operating status for the DSN rule.
5. Click **Finish** to confirm your decision. You return to the DNS Rule list page. The status of the DNS rule appears as "Active".

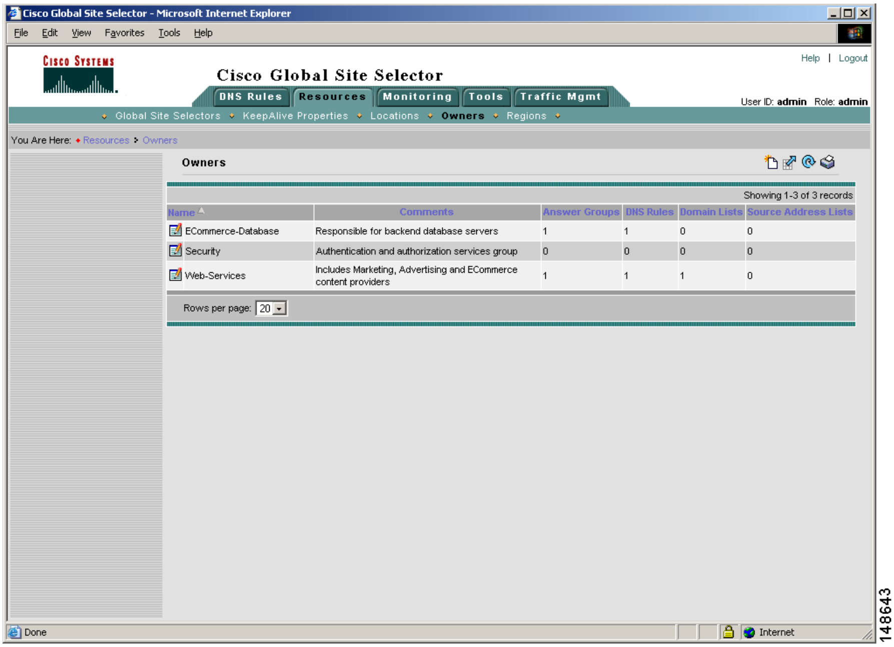
Suspending or Reactivating All DNS Rules Belonging to an Owner

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:

1. From the primary GSSM GUI, click **Resources** tab.
2. Click the **Owners** navigation link. The Owners list page appears (Figure 7-21).

Figure 7-21 Owners List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Owners
Done
Internet
148643

Owners

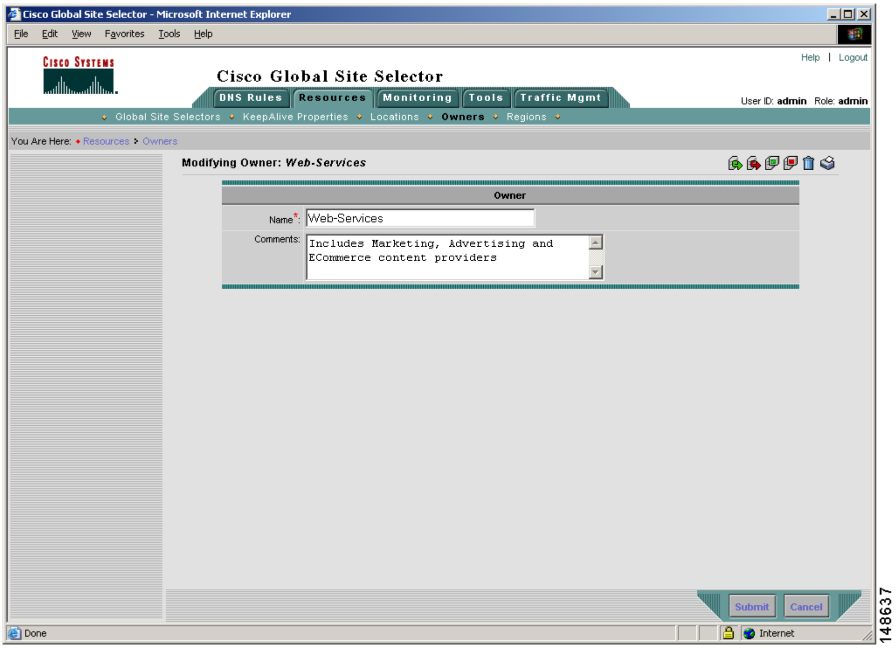
Showing 1-3 of 3 records

Name	Comments	Answer Groups	DNS Rules	Domain Lists	Source Address Lists
ECommerce-Database	Responsible for backend database servers	1	1	0	0
Security	Authentication and authorization services group	0	0	0	0
Web-Services	Includes Marketing, Advertising and ECommerce content providers	1	1	1	0

Rows per page: 20

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 (Figure 7-22).

Figure 7-22 Modifying Owners Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Owners
Submit
Cancel
Done
Internet
148637

Modifying Owner: *Web-Services*

Owner

Name*: Web-Services

Comments: Includes Marketing, Advertising and ECommerce content providers

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. Refer to the *Global Site Selector Administration Guide* for details.

To delete a DNS rule:

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

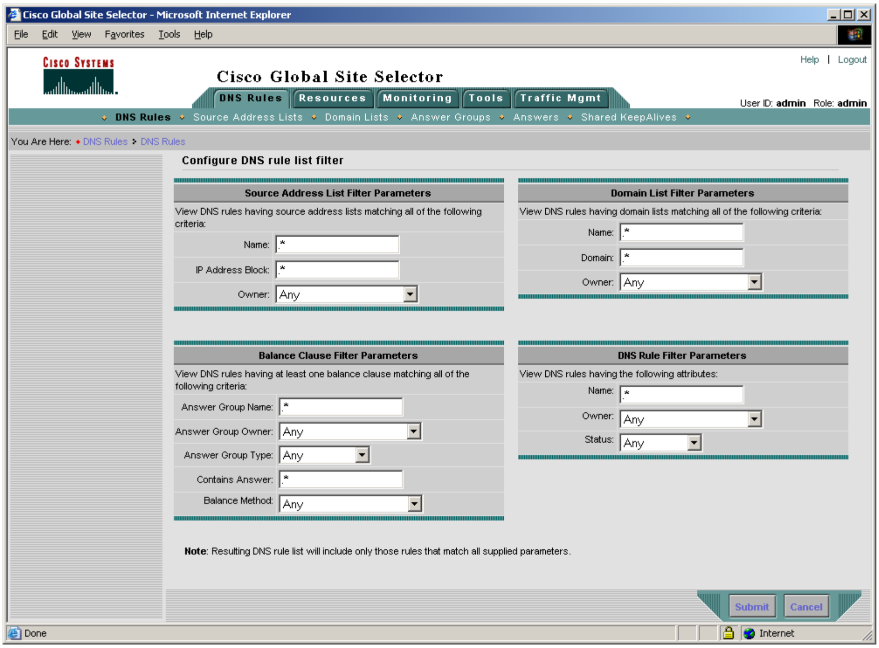
As your GSS network grows, so will your collection of DNS rules for handling traffic to and from your network. In time, it may become difficult to locate the rules that you need. For that reason, the primary GSSM GUI provides filters that you can apply to your DNS rules to view only those rules that 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:

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 (Figure 7-23).

Figure 7-23 Configure DNS Rule List Filter Details Page



User ID: admin Role: admin

You Are Here: DNS Rules > DNS Rules

Configure DNS rule list filter

Source Address List Filter Parameters

View DNS rules having source address lists matching all of the following criteria:

Name: .*

IP Address Block: .*

Owner: Any

Domain List Filter Parameters

View DNS rules having domain lists matching all of the following criteria:

Name: .*

Domain: .*

Owner: Any

Balance Clause Filter Parameters

View DNS rules having at least one balance clause matching all of the following criteria:

Answer Group Name: .*

Answer Group Owner: Any

Answer Group Type: Any

Contains Answer: .*

Balance Method: Any

DNS Rule Filter Parameters

View DNS rules having the following attributes:

Name: .*

Owner: Any

Status: Any

Note: Resulting DNS rule list will include only those rules that match all supplied parameters.

3. To filter your list by any of the properties displayed on the Filter List page, enter 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 7-1 DNS Rules Filter Parameters

Parameter	Description	Selection Examples
Source Address List Filter Parameters		
Name	Name assigned to a source address list associated with the DNS rule	VIP1 VIP* NameServerList
IP Address Block	IP address or address block assigned to a source address list associated with the DNS rule	192.168.110.100 192.168.*
Owner	Name of the owner assigned to the source address list associated with the DNS rule	Any System Education
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
Balance Clause Filter Parameters		
Answer Group Name	Name assigned to an answer group associated with the DNS rule	VIP_answer_Group_1 VIP_answer_Group_2 VIP_*

Table 7-1 DNS Rules Filter Parameters (continued)

Parameter	Description	Selection Examples
Answer Group Owner	Name of the owner assigned to the answer group associated with the DNS rule	Any System HR
Answer Group Type	Type of answer group associated with the DNS rule	CRA Name Server VIP
Contains Answer	Answer belonging to an answer group associated with the DNS rule	192.161.1.2 192.168.*
Balance Method	Type of balance method (such as boomerang and ordered list) associated with the DNS rule	Boomerang Hashed Least Loaded Order List Round-Robin Weighted Round-Robin
DNS Rule Filter Parameters		
Name	Name of the DNS rule	Cisco_Rule Cisco*
Owner	Name of the owner assigned to the DNS rule	Any System Sales
Status	Status of the DNS rule, either active or suspended	Any Active Suspended

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

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:

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.

Delegation 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. The A records which define the name servers within the domain are frequently called glue records.

Example 7-1 provides an example of a DNS zone configuration file for a fictitious cisco.com domain that has been modified to delegate primary DNS authority for three domains to two GSS devices. Relevant lines are shown in bold type.

In Example 7-1, the delegated domains are as follows:

- www.cisco.com
- ftp.cisco.com
- media.cisco.com

The GSS devices are as follows:

- gss1.cisco.com
- gss2.cisco.com

Example 7-1 Sample BIND Zone Configuration File Delegating GSSs

```
cisco.com. IN SOA ns1.cisco.com. postmaster.cisco.com. (
        2001111001; serial number
        36000; refresh 10 hours
        3600    ; retry   1  hour
        3600000; expire  42 days
        360000; minimum 100 hours )

; Corporate Name Servers for cisco.com
        IN  NS  ns1.cisco.com.
        IN  NS  ns2.cisco.com.
ns1     IN  A   192.168.157.209
ns2     IN  A   192.168.150.100

; Sub-domains delegated to GSS Network
www     IN  NS  gss1.cisco.com.
        IN  NS  gss2.cisco.com.
media   IN  CNAME www
ftp     IN  NS  gss1.cisco.com.
        IN  NS  gss2.cisco.com.
```

```
; “Glue” A records with GSS interface addresses
;       Cisco GSS Dallas
gss1    IN  A   172.16.2.3
;       Cisco GSS London
gss2    IN  A   192.168.3.6
.
.
```

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

Where To Go Next

If you plan to use DNS sticky for your global server load balancing, configure local or global DNS sticky for GSS devices in your network. Refer to Chapter 8, Configuring DNS Sticky for details.

If you plan to use network proximity for your global server load balancing, configure proximity for GSS devices in your network. Refer to Chapter 9, Configuring Network Proximity for details.

CHAPTER 8

Configuring DNS Sticky

This chapter describes how to configure a GSS to support 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
- Configuring Sticky Using the Primary GSSM GUI
- Configuring Sticky Using the GSS CLI
- Disabling DNS Sticky Locally on a GSS for Troubleshooting

Note 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. Refer to Chapter 10, 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 responses to the requesting client D-proxy, assuming that the original 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 includes 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: 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 IP address may also be some form of a sticky global netmask if the global subnet mask is set to a value other than the default of 255.255.255.255.

The sticky database stores the answer to each request that the DNS rule matches, which may be for a single domain (including wildcard expressions) or a configured list of domains. These components make up each sticky database key that the GSS uses for the look up, storage, and persistence of stickiness for DNS responses.

The primary GSSM supports the creation of sticky groups which 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 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 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 five 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 five 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 includes 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, as well as 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”.

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 due to a sticky database overflow because 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.

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 containing the most recently configured answer based on 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:

- Configure sticky DNS rules for one domain only. Avoid using the By Domain List selection for the sticky method unless absolutely necessary.
- Avoid the use of 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 the use of low DNS TTL values in a sticky balance clause.

Communicating in the Sticky Peer Mesh

To successfully pass packets between GSS peers in the sticky mesh, ensure 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 three 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.

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 a **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 a **gss reload** CLI command to perform a cold restart of the local GSS node.
- Select 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 anytime 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 8-1 provides a quick overview of the steps required to configure the GSS for DNS sticky operation, both local and global DNS sticky. Each step includes the primary GSSM 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 8-1 DNS Sticky Configuration Quick Start

Task and Command Example

1. If you are using global sticky with multiple GSS devices, log in to the CLI of each GSS in the mesh, enable privileged EXEC mode, and synchronize its system clock with an NTP server.
For example:
`gss1.example.com> enable`
`gss1.example.com# config`
`gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3`
`gss1.example.com(config)# ntp enable`

2. Log in to the primary GSSM GUI.
3. Click the **Traffic Mgmt** tab, then click the **Sticky** navigation link to access the Global Sticky Configuration details page.
4. At the State option, click one of the option buttons to enable DNS sticky for the GSS network: • **Local**—Enables DNS sticky for each active GSS device on a local level only. • **Global**—Enables DNS sticky across the entire GSS network. All local sticky features are in operation in addition to sharing sticky database information between all GSS peers in the network.

Table 8-1 DNS Sticky Configuration Quick Start (continued)

Task and Command Example
5. To modify one or more of the DNS sticky configuration default settings in the Global Sticky Configuration details page, perform the following steps: **a.** In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses. You can use this parameter as an attempt 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.
6. To configure inter-GSS global sticky mesh settings in the Global Sticky Configuration details page, perform 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.

Table 8-1 DNS Sticky Configuration Quick Start (continued)

Task and Command Example
8. Access the DNS Rule 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 is a new DNS rule) or the **Modify DNS Rule Using Rule Builder Interface** icon (if this is an existing DNS rule) 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.

Table 8-1 DNS Sticky Configuration Quick Start (continued)

Task and Command Example

9. Enable DNS sticky in a DNS rule using the DNS Rule Builder. Define the following DNS rule configuration information as follows:

   a. At the Select Sticky Method option, choose one of the following sticky selections:

      By Domain— Enables DNS stickiness on a matching hosted domain.

      By Domain List—Enables DNS stickiness on a matching hosted domain list.

   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.

   c. For each balance clause that you want to perform DNS sticky load balancing, click the **Sticky Enable** checkbox.

Note The GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

10. (Optional) To group multiple D-proxy IP addresses as a single entry in the sticky database, log on to the CLI of the primary GSSM, enable privileged EXEC mode, access the global server load-balancing configuration mode, and use the **sticky group** command.

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

Synchronizing the GSS System Clock with an NTP Server

If you are using global sticky in your GSS network, you must synchronize the clocks of all GSS devices in the mesh for a GSS to be able 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 (greater than a three minute difference), that GSS will ignore update messages from other GSS devices until you synchronize its system clock.

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 operating 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, refer to 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:

ntp-server *ip_or_host*

The *ip_or_host* variable specifies the IP address or host name of the NTP time server in your network that provides the clock synchronization. You can specify a maximum of four IP addresses or host names. Enter the IP address in dotted-decimal notation (for example, 172.16.1.2) or a mnemonic host name (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:

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
gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
gss1.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 includes the following procedures:

- 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.

Note here that 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:

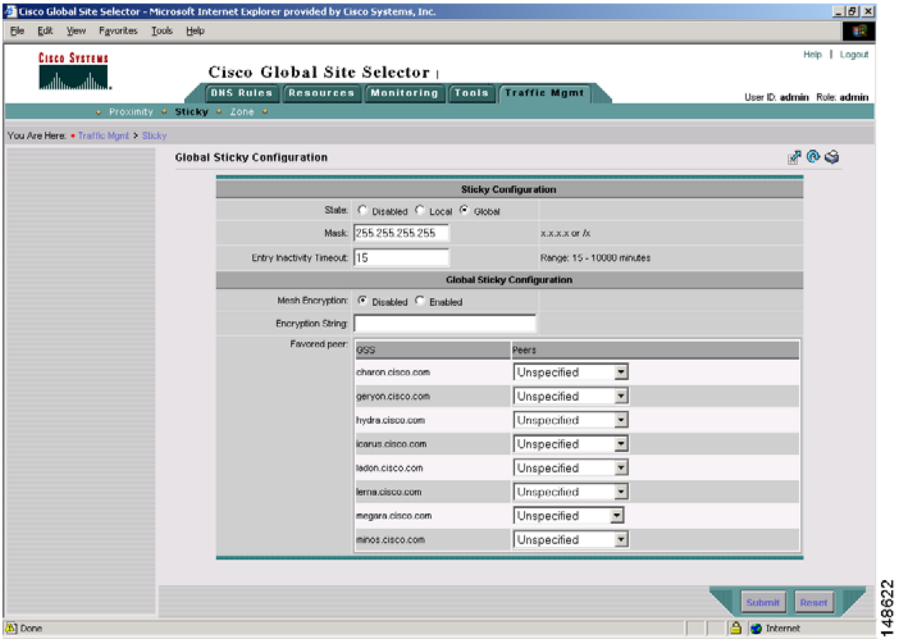
- Sticky is enabled for either global or local use. In the GUI, select **Global** or **Local** for the State option in the Global Sticky Configuration details page.
- A sticky method option (domain or domain list) is selected. In the GUI, use the DNS Rule Builder and select **By Domain** or **By Domain 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:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Sticky** navigation link. The Global Sticky Configuration details page appears (Figure 8-1).

Figure 8-1 Global Sticky Configuration Details Page—Sticky Configuration Fields


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: Traffic Mgmt > Sticky
Submit
Reset
Done
Internet
148622

Global Sticky Configuration

Sticky Configuration

State: ○ Disabled ○ Local ● Global

Mask: 255.255.255.255 x.x.x.x or /x

Entry Inactivity Timeout: 15 Range: 15 - 10080 minutes

Global Sticky Configuration

Mesh Encryption: ● Disabled ○ Enabled

Encryption String:

Favored peer:

GSS	Peers
charon.cisco.com	Unspecified
geryon.cisco.com	Unspecified
hydra.cisco.com	Unspecified
icarus.cisco.com	Unspecified
ladon.cisco.com	Unspecified
lerna.cisco.com	Unspecified
megara.cisco.com	Unspecified
minos.cisco.com	Unspecified

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 of the GSS devices 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 as an attempt to increase the number of clients that the sticky database can support. This mask is applied to the client source IP address before accessing the sticky database. Enter the subnet mask in 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 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 Entry Inactivity Timeout field, enter the maximum time period that an unused answer remains valid in the sticky database. This value defines the sticky database entry age-out process. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky 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. Enter a value from 15 to 10080 minutes (168 hours), specified in 5 minute intervals (15, 20, 25, 30, up to 10080). 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.

Note The sticky inactivity timeout is accurate to within five 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 five minutes past the specified value.

6. 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, proceed to the "Configuring the Global Sticky Mesh" section.

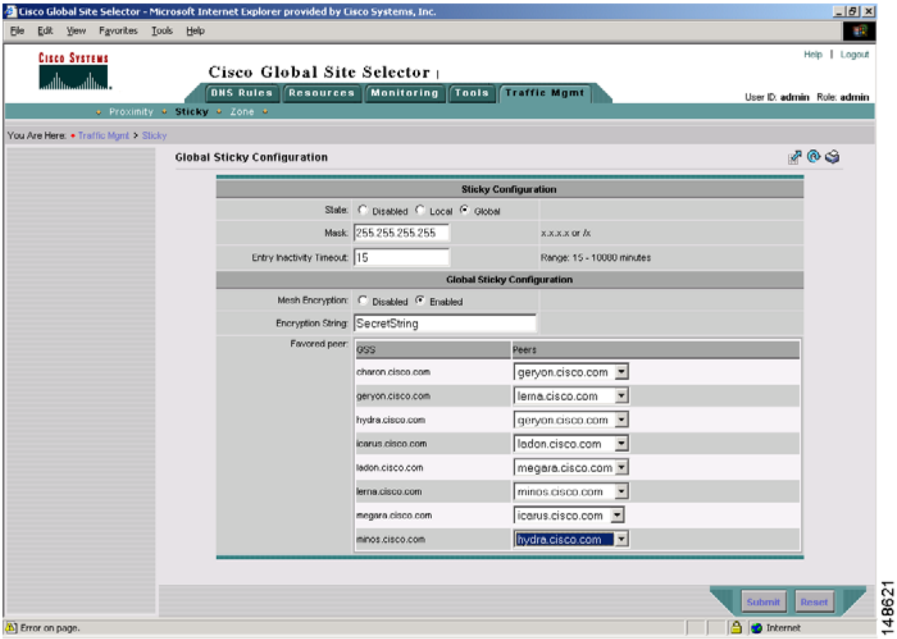
Configuring the Global Sticky Mesh

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:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Sticky** navigation link. The Global Sticky Configuration details page appears (Figure 8-2).

Figure 8-2 Global Sticky Configuration Details Page—Global Sticky Configuration Fields


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: Traffic Mgmt > Sticky
Submit
Reset
Error on page.
Internet
148621

Global Sticky Configuration

Sticky Configuration

State: ○ Disabled ○ Local ● Global

Mask: 255.255.255.255 x.x.x.x or /x

Entry Inactivity Timeout: 15 Range: 15 - 10000 minutes

Global Sticky Configuration

Mesh Encryption: ○ Disabled ● Enabled

Encryption String: SecretString

Favored peer:

GSS	Peers
charon.cisco.com	geryon.cisco.com
geryon.cisco.com	lerna.cisco.com
hydra.cisco.com	geryon.cisco.com
icarus.cisco.com	ladon.cisco.com
ladon.cisco.com	megara.cisco.com
lerna.cisco.com	minos.cisco.com
megara.cisco.com	icarus.cisco.com
minos.cisco.com	hydra.cisco.com

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.

    - **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. To authenticate communication between GSS peers 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 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. Enter an unquoted text string with a maximum of 32 characters and no spaces.

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 a:

   - Reload
   - Power up
   - **gss stop** and **gss start** CLI command sequence
   - **gss reload** CLI command
   - **sticky stop** and **sticky start** CLI command sequence
   - When you select 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 includes 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 is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

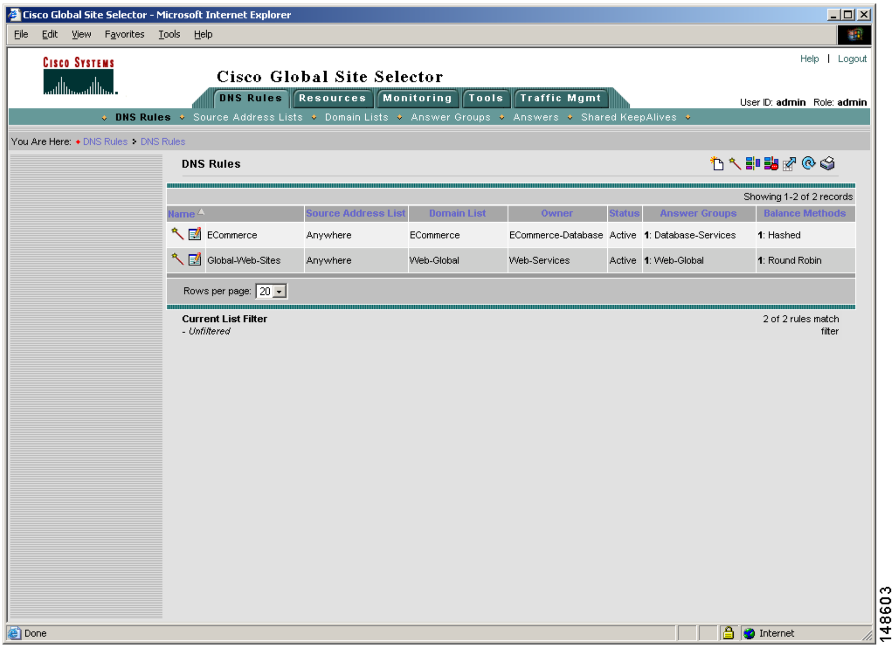
Note If you use DNS sticky and network proximity in your DNS rule, stickiness always takes precedence over proximity. When a valid sticky answer exists for a given DNS rule match, the GSS does not consider proximity when returning an answer to a client D-proxy.

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:

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, then click the **DNS Rules** navigation link. The DNS Rules list page appears (Figure 8-3).

Figure 8-3 DNS Rules List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
DNS Rules Source Address Lists Domain Lists Answer Groups Answers Shared KeepAlives
You Are Here: DNS Rules > DNS Rules
Done
Internet
148603

DNS Rules

Showing 1-2 of 2 records

Name	Source Address List	Domain List	Owner	Status	Answer Groups	Balance Methods
ECommerce	Anywhere	ECommerce	ECommerce-Database	Active	1: Database-Services	1: Hashed
Global-Web-Sites	Anywhere	Web-Global	Web-Services	Active	1: Web-Global	1: Round Robin

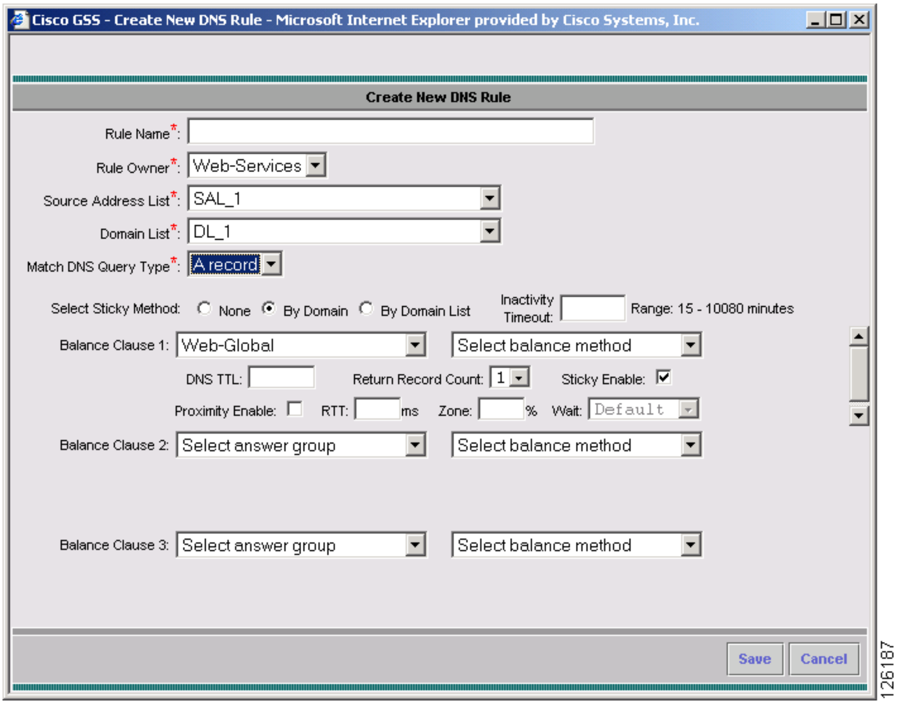
Rows per page: 20

Current List Filter
- *Unfiltered*

2 of 2 rules match filter

3. Click the **Open Rule Builder** icon. The Create New DNS Rule page opens in a separate window (Figure 8-4).

Figure 8-4 Create New DNS Rule Window



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Create New DNS Rule

Rule Name*:

Rule Owner*: Web-Services

Source Address List*: SAL_1

Domain List*: DL_1

Match DNS Query Type*: A record

Select Sticky Method: ○ None ● By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes

Balance Clause 1: Web-Global Select balance method

DNS TTL: Return Record Count: 1 Sticky Enable: ☑

Proximity Enable: □ RTT: ms Zone: % Wait: Default

Balance Clause 2: Select answer group Select balance method

Balance Clause 3: Select answer group Select balance method

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. To enable or disable sticky globally for the DNS rule, at the Select Sticky Method option, choose 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. To 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, specify a value in the Inactivity Timeout field. 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. Enter a value from 15 to 10080 minutes, defined in 5 minute intervals (15, 20, 25, 30 up to 10080).

Note The sticky inactivity timeout is accurate to within five 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 five minutes past the specified value.

7. At the Balance Clause 1 heading:
   - Select 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.
   - Select 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 outlined in the "Building DNS Rules Using the DNS Rule Builder" section of Chapter 7, Building and Modifying DNS Rules. Select 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 is also true 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 discusses 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 for ease of sticky y group creation through automation scripts. You can also use the CLI of each GSS in your network to perform sticky database activities on an individual GSS basis, 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 includes the following procedures:

- 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. Refer to 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:

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 host name or IP address of the GSS to access the CLI.

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

   For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, refer to 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 includes 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

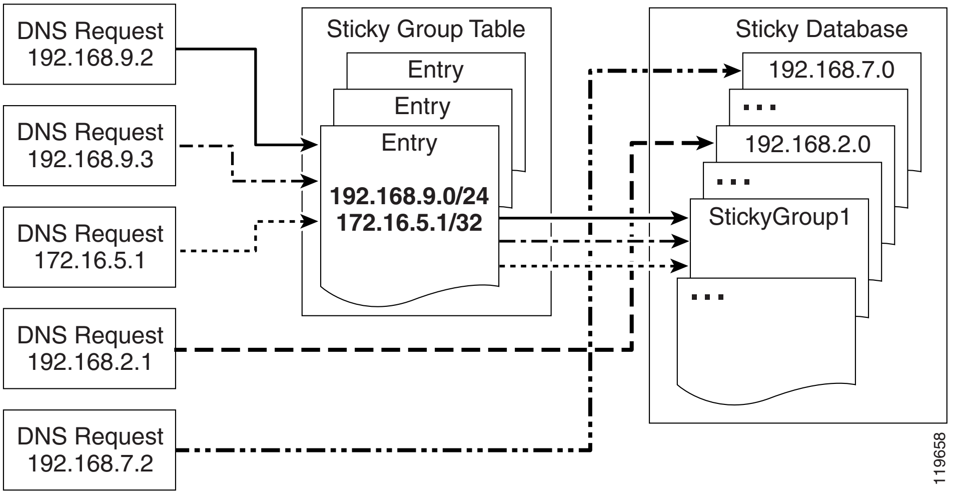
You create sticky groups from the primary GSSM CLI to obtain better scalability of your configuration and to allow for ease of sticky group creation through automation scripts. The primary GSSM supports a maximum of 800 sticky groups. Each sticky group contains one to 30 blocks of IP addresses and subnet masks (in dotted-decimal notation).

The grouping of D-proxy IP addresses in the sticky database provides you with a method 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, referred to as proxy hopping, has implications for sticky 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 provides you with a mechanism to globally group sets of D-proxies together to solve this proxy hopping problem.

In addition to creating DNS sticky groups of multiple D-proxy IP addresses from the CLI, you can configure a global netmask 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 IP address (255.255.255.255) and the global netmask as the key to look up in the DNS sticky database. The default global mask is 255.255.255.255.

Figure 8-5 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 8-5 Locating a Grouped Sticky Database Entry



Creating a DNS Sticky Group

To create a DNS sticky group, use 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:

sticky group *groupname* **ip** *ip-address* **netmask** *netmask*

The options and variables are:

- *groupname*—Enter a unique alphanumeric name for the DNS sticky group, with a maximum of 80 characters. Use only alphanumeric characters and the underscore ("_") character.
- **ip** *ip-address*—The IP address block specified in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmask*—The subnet mask of the IP address block specified in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to create a sticky group called *StickyGroup1* with an IP address block of 192.168.9.0 255.255.255.0:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# sticky group StickyGroup1 ip
192.168.9.0 netmask 255.255.255.0
```

Reenter the **sticky group** command if you want to perform one of the following tasks:

- Add multiple IP address blocks to a DNS sticky group
- Create additional DNS sticky groups

Each sticky group can have a maximum of 30 blocks of defined IP addresses and subnet masks. The GSS prohibits duplication of IP addresses and subnet masks among DNS sticky groups.

Deleting a Sticky Group IP Address Block

To delete a previously configured IP address block from a sticky group, use the **no** form of the **sticky group ip** command. For example:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no sticky group StickyGroup1 ip
192.168.3.0 netmask 255.255.255.0
```

Deleting a Sticky Group

To delete a sticky group, use the **no** form of the **sticky group** command. For example:

```
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 in special circumstances when you want to remove all entries from the sticky database in order to have an empty database. Ensure that you want to permanently delete entries from the sticky database before you enter this command. You cannot retrieve sticky database entries once they are deleted.

To view the entries in the sticky database to identify the sticky entries that you want to delete, use the **show sticky database** command (refer to the "Displaying Sticky Database Status" section in Chapter 10, 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:

> **sticky database delete** {**all** | **answer** {*name/ip_address*} | **domain** {*name*} | **domain-list** {*name*} | **group** {*name*} | **inactive minimum** {*minutes*} **maximum** {*minutes*} | **ip** {*ip_address*} **netmask** {*netmask*} | **rule** {*rule_name*}}

The options and variables are:

- **all**—Removes all entries from the sticky database memory. The prompt `Are you sure?` appears to confirm the deletion of all database entries. Specify **y** to delete all entries or **n** to cancel the deletion operation.
- **answer** *name/ip_address*—Removes all sticky entries related to a particular answer. Specify the name of the answer. If there is no name for the answer, specify the IP address of the sticky answer in dotted-decimal notation (for example, 192.168.9.0).
- **domain** *name*—Removes all sticky entries related to a domain. Specify the exact name of a previously created domain.
- **domain-list** *name*—Removes all sticky entries related to a domain list. Specify the exact name of a previously created domain list.
- **group** *name*—Removes all sticky entries related to a sticky group. Specify the exact name of a previously created sticky group.
- **inactive minimum** *minutes* **maximum** *minutes*—Removes all sticky entries that have not received a lookup request by a client D-proxy in the specified minimum and maximum time interval. 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 the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **rule** *rulename*—Removes all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

For example, to remove the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gss1.example.com# sticky database delete ip 192.168.8.0 netmask
255.255.255.0
```

Dumping Sticky Database Entries

The GSS automatically dumps sticky database entries to a backup file on disk approximately every 20 minutes. The GSS uses this backup file to initialize the sticky database upon system restart or reboot to enable the GSS to recover the contents of the database. When global sticky is enabled, the GSS restores from the database dump file anytime it reenters the mesh and cannot retrieve the sticky database contents from a GSS peer in the mesh.

If desired, 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. Refer to the *Cisco Global Site Selector Administration Guide* for details about displaying the contents of a file.

The GSS includes a number of options to 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:

sticky database dump {*filename*} **format** {**binary** | **xml**} **entry-type** {**all** | **group** | **ip**}

The options and variables are:

- *filename*—The name of the output file containing 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. Select 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:
  - **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.

Note Dumping sticky database entries in XML format can be a resource intensive operation and may take from two to four minutes to complete depending on the size of the sticky database and the GSS platform in use. We recommend that you do not perform a sticky database dump in XML format during the routine operation of the GSS to avoid a degradation in performance.

- **entry-type**—Specifies the type of sticky database entries to dump. The valid entries are:
  - **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.

gss1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump is in progress...
Sticky Database has dumped 15678 of 34512 entries

gss1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump completed. The number of dumped entries: 34512
gss1.example.com#
```

When the dump finishes, a "completed" message displays and the CLI prompt reappears.

Running a Periodic Sticky Database Backup

You can instruct the GSS to dump sticky database entries to an output file on the GSS disk prior to 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 prior to shutting 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:

sticky database periodic-backup now

For example, enter:

```
gss1.example.com# sticky database periodic-backup now
```

Loading Sticky Database Entries

The GSS supports the loading and merging of sticky database entries from a file into the existing sticky database in GSS memory. The 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:

sticky database load *filename*

Note If you prefer to load and replace all sticky database entries from a GSS instead of merging the entries with the existing sticky database, first enter the **sticky database delete all** command to remove all entries from sticky database memory before you enter the **sticky database load** command.

Specify the name of the sticky database file to load and merge with the existing sticky database on the GSS device. The file must be in binary format for loading into GSS memory (see the "Dumping Sticky Database Entries" section). Use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the sticky database file to the GSS from a remote GSS.

This example shows how to load and merge the entries from the *GSS3SDB* file with the existing entries in the GSS sticky database:

```
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 a **gss restart** CLI command to restart the GSS software.
- Enter a **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
```

CHAPTER 9

Configuring Network Proximity

This chapter describes how to configure a Global Site Selector 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

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. Refer to Chapter 10, 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 probing device, a Cisco IOS-based router, located in each proximity zone to gather round-trip time (RTT) metric information measured between the requesting client's D-proxy and the zone. Each GSS directs client requests to an available server with the lowest RTT value.

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

This section describes the major functions in GSS network proximity:

- Proximity Zones
- Probe Management and Probing
- Proximity Database
- Example of Network Proximity

Proximity Zones

A network can be logically partioned into "zones" based on the arrangement of devices and network partioned 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 probing device that is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one probing device to a requesting D-proxy.

A location is a method to logically group devices in data centers for administrative purposes. A location can represent a physical point, such as a building or a rack. When you use the GSS to perform network proximity, each location must be assigned to a zone. In addition, you assign each answer used in a GSS proximity DNS rule to a location that is associated with a zone. This configuration hierarchy informs the GSS about resources when determining the most proximate answer.

Probe Management and Probing

Probe management is the intelligence behind each GSS device's interaction with the probing device in a zone. Within each zone, there must be at least one probing device and, optionally, a backup probing device. Upon failure of the primary probing device, the probes are redirected to the backup device. Once the primary probing device becomes available, probes are redirected back to the primary probing device.

The GSS uses Director Response Protocol (DRP) to communicate with the probing devices, called DRP agents, in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems. You can use any Cisco router as the probing device in a zone that is capable of supporting the DRP agent software and can measure ICMP, TCP, or path-probe RTT. The GSS communicates with the Cisco IOS-based router using the DRP RTT query and response method.

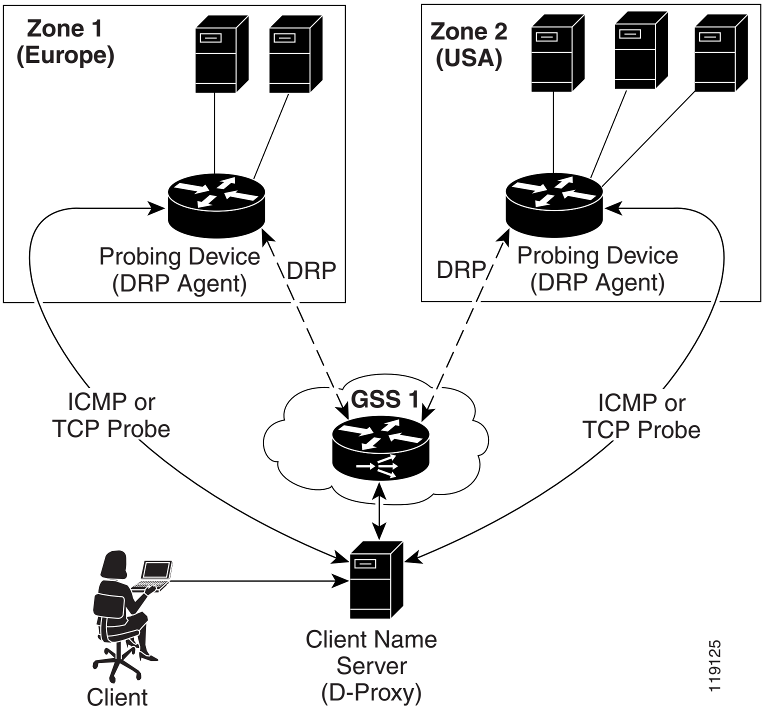
Each DRP agent accepts probing instructions from the GSS and returns probing results to the GSS based on the DRP protocol. DRP allows for the authentication of packets exchanged between the DRP agent and the GSS.

The GSS transmits DRP queries to one or more probing devices in the GSS network, instructing the DRP agent in the probing device to probe specific D-proxy IP addresses. Each probing device responds to the query by using a standard protocol, such as ICMP or TCP, to measure the RTT between the DRP agent in the zone and the IP address of the requesting client's D-proxy device.

When the GSS receives a request from a D-proxy, it decides if it can provide a proximate answer. If the GSS is unable to determine a proximate answer from the proximity database (PDB), it sends a probe to one or more probing devices to get proximity information between those probing devices and the new D-proxy. After the GSS receives the probing results, it adds the RTT information to the PDB.

Figure 9-1 illustrates the probing process between a GSS (DRP client) and a probing device (DRP agent).

Figure 9-1 DRP Communication in a GSS Network



The GSS supports two type of probing methods:

- **Direct Probing**—Direct probing occurs between the GSS and DRP agents when the GSS creates a dynamic entry in the PDB as the result of receiving a new D-proxy IP address. Direct probing also occurs when you specify alternative IP addresses as targets for the probing devices to obtain RTT data and add static entries in the PDB. The GSS initiates direct probing to the DRP agent when a request is made for a new D-proxy IP address entry. Through direct probing, the GSS automatically sends probe requests to the DRP agent in each zone to obtain initial probe information as quickly and efficiently as possible for the new entries in the PDB.
- **Refresh Probing**—The GSS periodically re-probes 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 proximity database (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 probing devices in every zone in the proximity network, and puts the results in the PDB.

For example, a GSS communicates with three zones to determine the most proximate answer and receives the following RTT values from the probing devices in each zone to a particular client D-proxy:

- Zone1 = 100 ms
- Zone2 = 120 ms
- Zone3 = 150 ms

From the three RTT values in the PDB, the GSS selects Zone1 as the most proximate zone for the client's D-proxy request because it has the smallest RTT value.

The GSS supports a maximum of 500,000 D-proxy IP address entries in the PDB table, both dynamic and static entries. The GSS creates dynamic entries in the PDB as the result of requests for new D-proxy IP addresses. If required, 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 which 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 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.

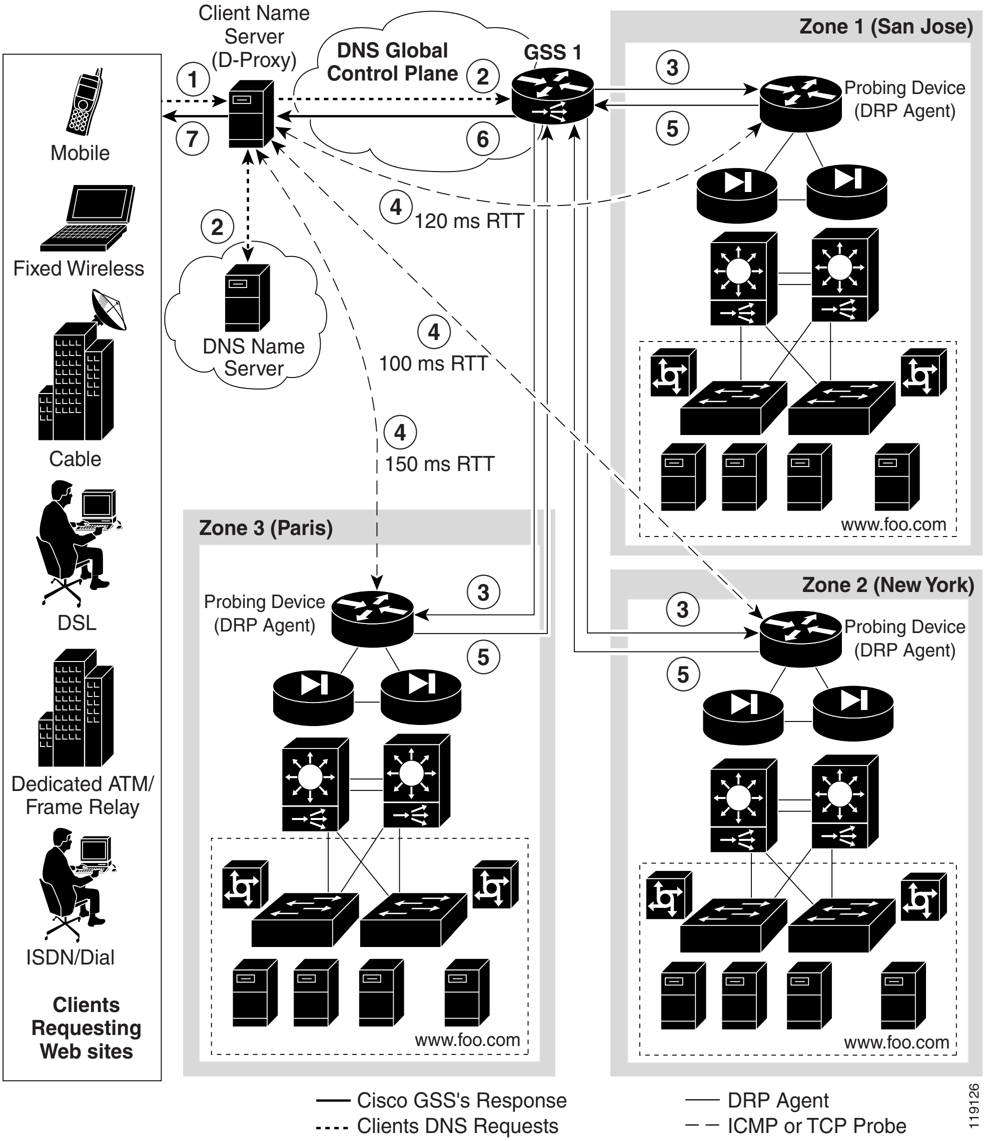
When the PDB reaches a maximum of 500,000 entries, the GSS does not add entries to the PDB and any new requests for answers result in a failure. The GSS tracks how many entries are dropped because the maximum limit has been reached. Once the number of PDB entries drops below 500,000, the GSS resumes adding new entries to the PDB.

Example of Network Proximity

The process outlined below describes how the GSS interacts with the probing devices in multiple zones to perform network proximity. See Figure 9-2 for an illustration of the following steps.

1. A client performs an HTTP request for *www.foo.com*. The content for this website is supported at three different data centers.
2. The DNS global control plane infrastructure processes this request and directs the client D-proxy to GSS 1. The GSS offloads the site selection process from the DNS global control plane. The client's local D-proxy queries GSS1 for the IP address associated with www.foo.com. The GSS accepts the DNS query.
3. If the request matches a proximity DNS rule configured on the GSS, the GSS performs an internal PDB lookup. If the lookup fails, the GSS sends DRP queries to the DRP agent configured for each zone.
4. When the DRP agent in each zone receives a DRP request, they measure RTT from their associated zone back to the requesting client D-proxy device, using either ICMP, TCP, or a path-probe.
5. After calculating DRP RTT metrics, the DRP agents send their replies to the GSS. The GSS sorts the DRP RTT replies from the DRP agents to identify the “best” (smallest) RTT metric. The DRP agent then returns the smallest RTT metric identifies the closest zone, which in Figure 9-2 is Zone 2 (New York).
6. The GSS returns to the client's local D-proxy one or more IP address records (DNS “A” resource records) that match the DNS rule, corresponding 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 corresponding to www.foo.com to the client that originated the request. The client transparently connects to the server in Zone 2 for www.foo.com.

Figure 9-2 Network Proximity Using the Cisco Global Site Selector



Proximity Network Design Guidelines

When developing your proximity network, plan it appropriately to ensure 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 zone configuration at any time by deleting or adding a zone, or by moving a zone from one location to another location.
- For each zone, identify the probing device and, optionally, the backup probing device. Each probing device represents the topological location of its associated zone and also reflects the zone's expected network behavior in terms of connectivity to the internet. The probing device is the DRP agent located within the zone.
- Each GSS network can contain a maximum of eight GSS devices. GSS devices can be added and deleted anytime. The GSS does not have to reside within a zone.
- To use proximity, you must:
  - 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, answers in the answer group must be contained in locations that are tied to a zone.

Network Proximity Quick Start Guide

Table 9-1 provides a quick overview of the steps required to configure the GSS for proximity network operation. Each step includes the primary GSSM 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 9-1 Proximity Configuration Quick Start

Task and Command Example

1. Log in to the CLI of each GSS in the network, enable privileged EXEC mode, and synchronize its system clock with an NTP server.
For example:
`gss1.example.com> enable`
`gss1.example.com# config`
`gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3`
`gss1.example.com(config)# ntp enable`

2. Configure a Cisco router as a DRP agent in one or more proximity zones.
3. Log in to the primary GSSM GUI.
4. Click the **Traffic Mgmt** tab, then click the **Zone** 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.
5. Click the **Proximity** navigation link to access the Proximity details page (Traffic Mgmt tab). At the State option, click the **Enabled** option button to globally enable proximity across the entire proximity network.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
6. If you need to modify one or more of the global proximity configuration default settings in the Proximity details page, perform the following: • 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 D-proxies 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 help 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 an 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.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
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 wish 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.
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 is a new DNS rule) or the **Modify DNS Rule Using Rule Builder Interface** icon (if this is an existing DNS rule) 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.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

12. Enable network proximity in a DNS rule using the DNS Rule Builder. Define the following DNS rule configuration information:

- **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) To 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, access the global server load-balancing configuration mode and create a proximity group at the primary GSSM CLI. Use 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
```

15. (Optional) To add static proximity entries to the PDB of a GSS device in your network, access the global server load-balancing configuration mode and use the **proximity assign** command to create 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”
```

Configuring a Cisco Router as a DRP Agent

When you enable DRP on a Cisco router, the router gains the additional functionality of operating as a DRP agent in the GSS network. A DRP agent can communicate with multiple GSSs and support multiple distributed servers.

This section includes the following background information about choosing and configuring the Cisco router in each proximity zone as a DRP agent:

- 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

To configure and maintain the DRP agent in the Cisco IOS-based router, perform the tasks described in the “Configuring IP Services” chapter, 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 only supported in Cisco IOS release 12.2T, 12.3, and later.

The GSS operates with Cisco IOS-based routers using the following DRP RTT probing methods: TCP (“DRP Server Agent”) and ICMP (“ICMP ECHO-based RTT probing by DRP agents”). “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 summarizes the steps required to configure a Cisco IOS-based router as a DRP agent:

1. Enable the DRP agent in the Cisco router.
2. Enable security for DRP by defining a standard access list that permits requests from 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 originating 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 Cisco router running IOS release 12.1, it is important to ensure the DRP authentication configuration is identical on both devices. For example, if you intend to perform DRP authentication between a GSS and a Cisco IOS 12.1 router, ensure that you properly enable and configure authentication on both devices. The same is true if you choose not to use DRP authentication; you disable authentication on both devices.In the case that you disable DRP authentication on a Cisco IOS 12.1 router but enable DRP authentication on a GSS, all measurement probes sent by a GSS to the Cisco IOS-based router will fail. This condition occurs because the Cisco IOS 12.1 router fails to recognize the DRP echo query packets sent by a GSS and the GSS cannot detect a potential failure of measurement packets sent to the router. In this case, the GSS identifies the Cisco IOS-based 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 DRP probe requests fails between the GSS and a Cisco router running IOS release 12.1, even when the GSS indicates that the router is ONLINE, verify the DRP authentication configurations on both the GSS and the Cisco router:

- To verify the DRP authentication configuration on the Cisco router running IOS release 12.1, enter the **show ip drp** command. If the line `Authentication is enabled, using "test" key-chain` appears in the output (where `"test"` is the name of your key-chain), DRP authentication is configured on the router. If this line does not appear in the output, DRP authentication is not configured.
- 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 Cisco router running 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 an 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. If the system clock of a GSS changes, this 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, refer to 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:

ntp-server *ip_or_host*

The *ip_or_host* variable specifies the IP address or host name of the NTP time server in your network that provides the clock synchronization. You can specify a maximum of four IP addresses or host names. Enter the IP address in dotted-decimal notation (for example, 172.16.1.2) or a mnemonic host name (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:

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
gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
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 probing device and a possible backup probing device. A zone can be geographically related to a continent, a country, or a major city. Each zone can include one or more locations. A location is a method to logically group collocated devices for administrative purposes.

During the proximity selection process, the GSS chooses the most proximate zones containing one or more valid answers based on RTT data received from probing devices configured in the zone. You can configure a proximity network with up to 32 zones.

This section includes the following procedures:

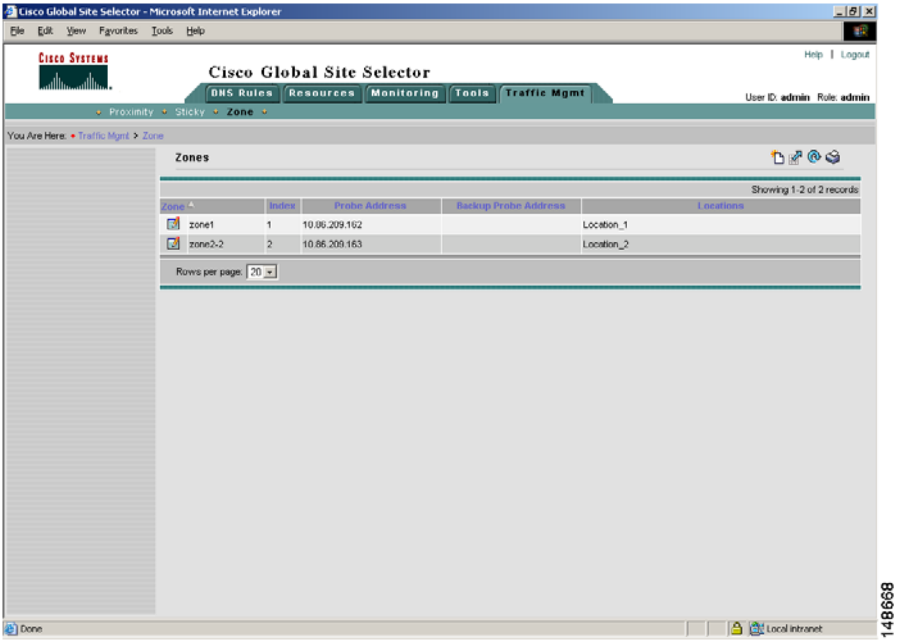
- Creating a New Proximity Zone
- Modifying a Proximity Zone
- Deleting a Proximity Zone
- Associating a Proximity Zone With a Location
- Associating a Proximity-Based Location with an Answer

Creating a New Proximity Zone

To create a proximity zone from the primary GSSM GUI:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zone** navigation link. The Zones list page appears (Figure 9-3).

Figure 9-3 Zones List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: Traffic Mgmt > Zone
Done
Local intranet
148668

Zones

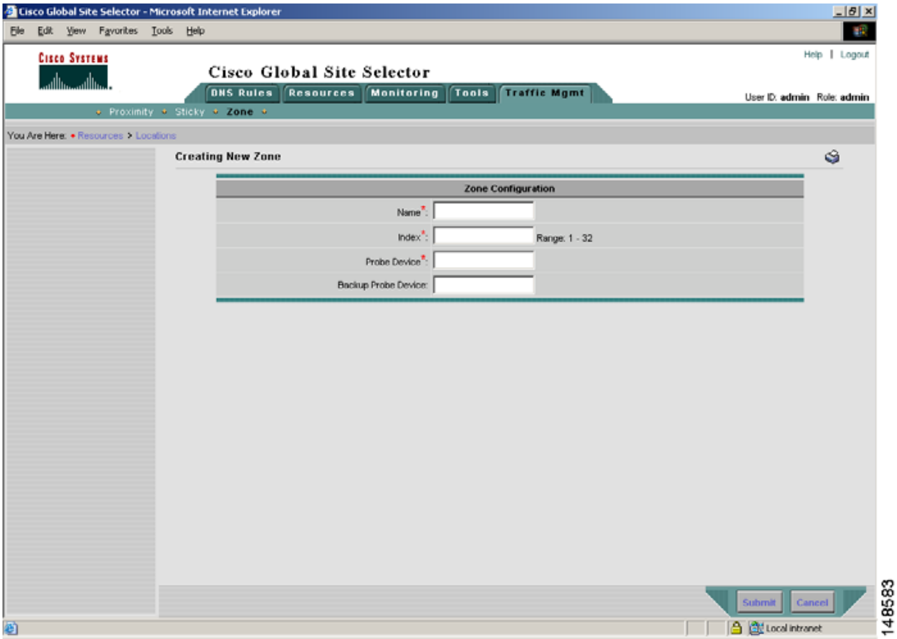
Showing 1-2 of 2 records

Zone	Index	Probe Address	Backup Probe Address	Locations
zone1	1	10.86.209.162		Location_1
zone2-2	2	10.86.209.163		Location_2

Rows per page: 20

3. Click the **Create Zone** icon. The Creating New Zone detail page appears (Figure 9-4).

Figure 9-4 Creating New Zone Detail Page



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.

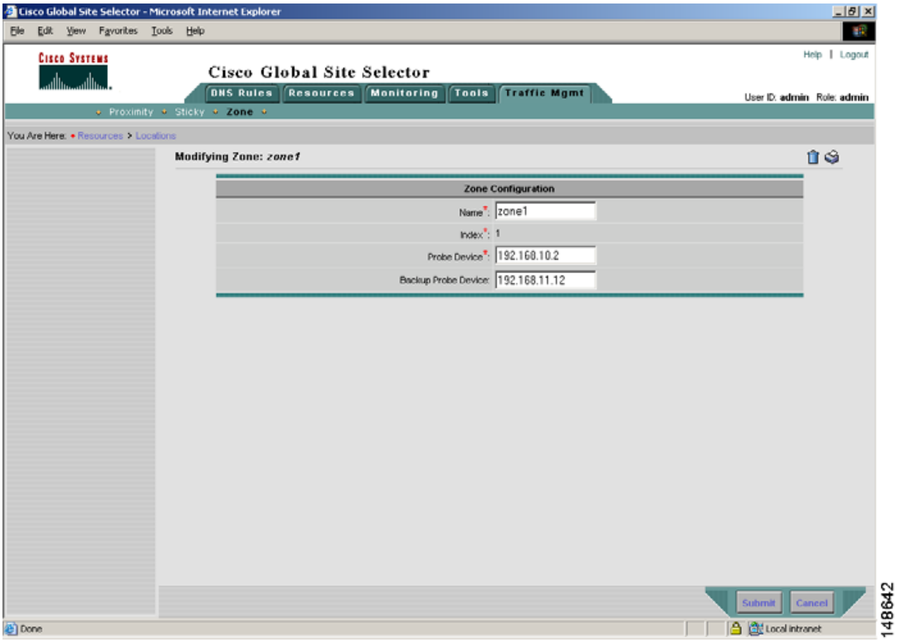
8. Click the **Submit** button to save your zone. You return to the Zones list page.

Modifying a Proximity Zone

To modify a proximity zone from the primary GSSM GUI:

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 you want to modify. The Modifying Zone details page appears (Figure 9-5).

Figure 9-5 Modifying Zone Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: Resources > Locations
Submit
Cancel
Done
Local intranet
148642

Modifying Zone: *zone1*

Zone Configuration

Name*: zone1
Index*: 1
Probe Device*: 192.168.10.2
Backup Probe Device: 192.168.11.12

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 containing 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:

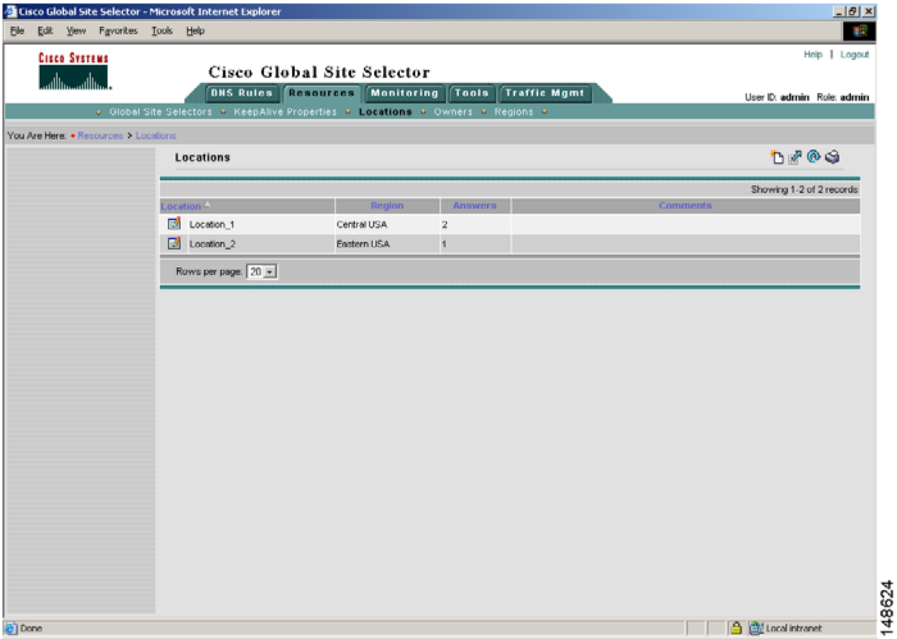
1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zones** navigation link. The Zones list page appears.
3. Click the **Modify Zone** icon located to the left of the zone that you want to delete. The Modifying Zone details page appears (see Figure 9-5).
4. Click the **Delete 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:

1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Locations** navigation link. The Locations list page appears (Figure 9-6).

Figure 9-6 Locations List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Locations
Done
Local intranet
148624

Locations

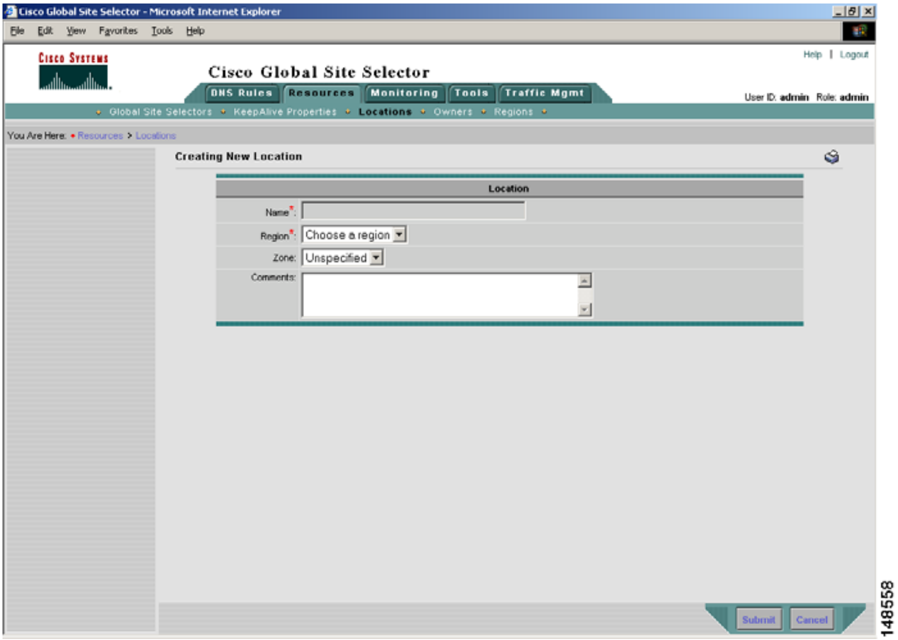
Showing 1-2 of 2 records

Location	Region	Answers	Comments
Location_1	Central USA	2	
Location_2	Eastern USA	1	

Rows per page: 20

3. Click either the **Create Location** icon (if this is a new location) or the **Modify Location** icon (if you are adding the proximity zone to an existing location). The Location details page appears (Figure 9-7). For details about creating a location, refer to Chapter 2, Configuring Resources.

Figure 9-7 Creating New Location Details Page



Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Global Site Selectors
KeepAlive Properties
Locations
Owners
Regions
You Are Here: Resources > Locations
Submit
Cancel
148558

Creating New Location

Location

Name*:

Region*: Choose a region

Zone: Unspecified

Comments:

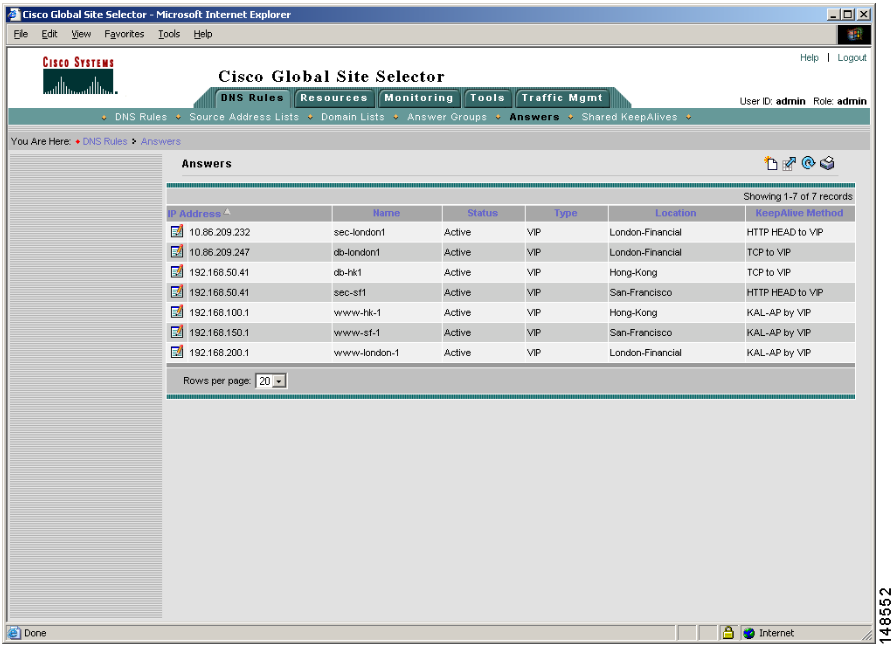
4. Click the **Zone** drop-down list and associate a zone with the location. There should be a logical connection between the zone and the location.
5. Click **Submit** to save changes to your location and return to the Locations list page.

Associating a Proximity-Based Location with an Answer

To assign a location that is associated with a proximity zone to an answer:

1. From the primary GSSM GUI, click the **DNS Rule** tab.
2. Click the **Answers** navigation link. The Answers list page appears (Figure 9-8).

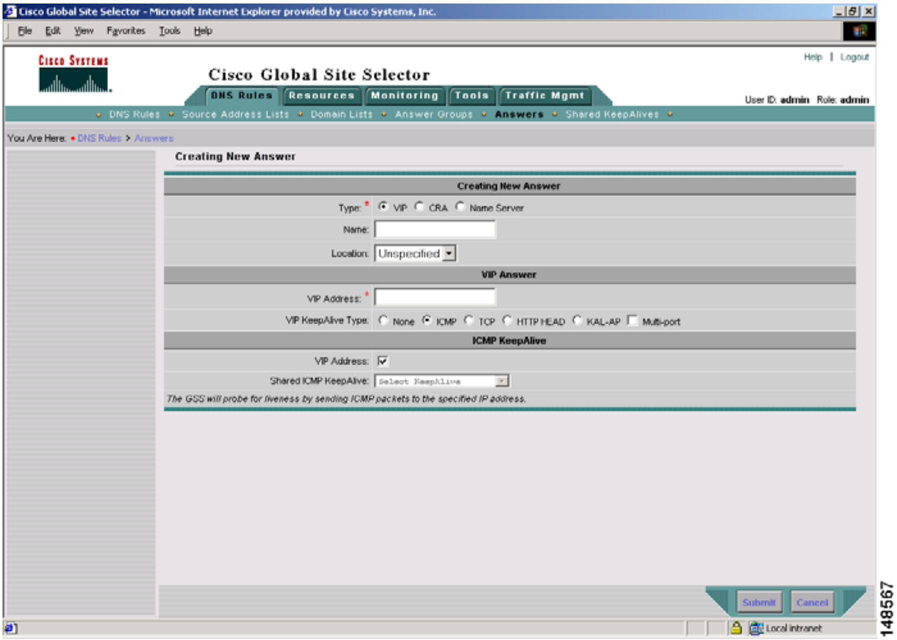
Figure 9-8 Answers List Page



IP Address	Name	Status	Type	Location	KeepAlive Method
10.86.209.232	sec-london1	Active	VIP	London-Financial	HTTP HEAD to VIP
10.86.209.247	db-london1	Active	VIP	London-Financial	TCP to VIP
192.168.50.41	db-hk1	Active	VIP	Hong-Kong	TCP to VIP
192.168.50.41	sec-sf1	Active	VIP	San-Francisco	HTTP HEAD to VIP
192.168.100.1	www-hk-1	Active	VIP	Hong-Kong	KAL-AP by VIP
192.168.150.1	www-sf-1	Active	VIP	San-Francisco	KAL-AP by VIP
192.168.200.1	www-london-1	Active	VIP	London-Financial	KAL-AP by VIP

3. Click either the **Create Answer** icon (if this is a new answer) or the **Modify Answer** icon (if you are adding the location to an existing answer). The Answer details page appears (Figure 9-9).

Figure 9-9 Creating New Answer Details Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Submit
Cancel
Local intranet
148567

Creating New Answer

Creating New Answer

Type: * ● VIP ○ CRA ○ Name Server

Name:

Location: Unspecified

VIP Answer

VIP Address: *

VIP KeepAlive Type: ○ None ● ICMP ○ TCP ○ HTTP HEAD ○ KAL-AP □ Multi-port

ICMP KeepAlive

VIP Address: ☑

Shared ICMP KeepAlive: Select KeepAlive

The GSS will probe for liveness by sending ICMP packets to the specified IP address.

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, select 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 discusses how to configure the GSS for network proximity operation from the primary GSSM GUI and how to add proximity to a DNS rule in the DNS Rule Builder. It includes the following procedures:

- Configuring Proximity
- Creating DRP Keys
- Deleting DRP Keys
- Using the DNS Rule Builder to Add Proximity to a DNS Rule

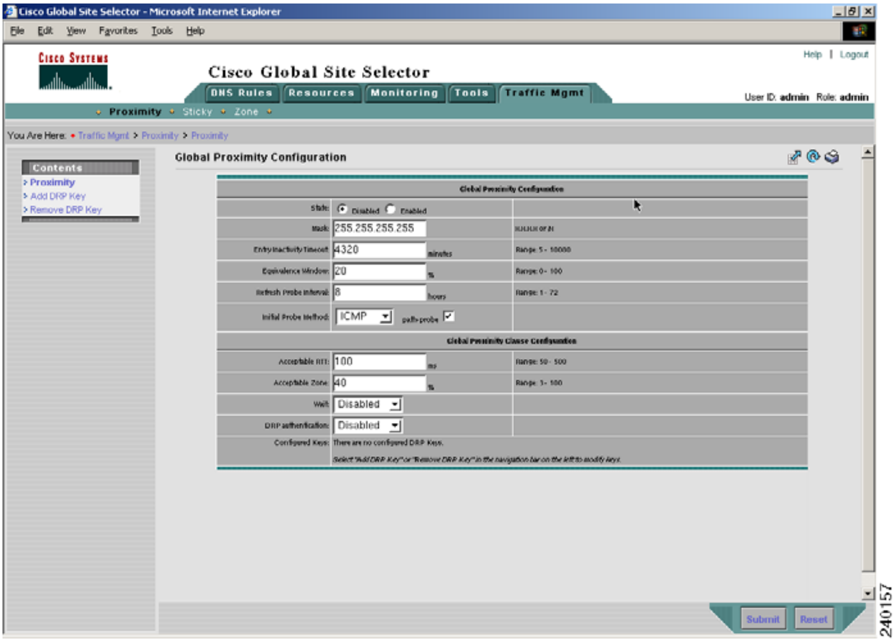
Configuring Proximity

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:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (Figure 9-10).

Figure 9-10 Global Proximity Configuration Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: Traffic Mgmt > Proximity > Proximity
Contents
Proximity
Add DRP Key
Remove DRP Key
Submit
Reset
240157

Global Proximity Configuration

Global Proximity Configuration		
State:	● Disabled ○ Enabled	
Mask:	255.255.255.255	x.x.x.x or /n
Entry Inactivity Timeout:	4320 minutes	Range: 5 - 10080
Equivalence Window:	20 %	Range: 0 - 100
Refresh Probe Interval:	8 hours	Range: 1 - 72
Initial Probe Method:	ICMP path-probe ☑	
Global Proximity Clause Configuration		
Acceptable RTT:	100 ms	Range: 50 - 500
Acceptable Zone:	40 %	Range: 1 - 100
Wait:	Disabled	
DRP authentication:	Disabled	
Configured Keys:	There are no configured DRP Keys. *Select "Add DRP Key" or "Remove DRP Key" in the navigation bar on the left to modify keys.*	

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 as an attempt 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 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. This value defines the PDB entry age-out process. Once an entry reaches the inactivity time, the GSS removes the selected dynamic entries from the PDB. Enter a value from 5 to 10080 minutes (168 hours). The default value is 4320 minutes (72 hours).
6. 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. 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 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. Enter an equivalence window value from 0 to 100 percent. The default value is 20 percent.
7. 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.

8. In the Initial Probe Method drop-down list, specify the type of probe method used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the Cisco 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.
    - **TCP**—The probing device uses the TCP SYN-ACK and RST handshake sequence to probe the user-specified TCP port and measure the RTT between the probing device and the D-proxy. You can configure the source and destination TCP ports on the Cisco router.
    - **ICMP**—The probing device uses ICMP echo request and response to measure the RTT between the probing device and the D-proxy.
    - **path-probe**—This is used as a fallback method for ICMP/TCP probes and cannot be selected as the initial probe method. It is only supported on the GSS acting as a DRP agent and by default, is not enabled.

      When the GSS fails to receive the minimum acceptable RTT metrics from the DRP agents, it sends a query message to the probing devices configured for each zone instructing the DRP agent running on the GSS to probe using the path-probe method instead. If at least one of the DRP agents returns RTT using the legacy ICMP/TCP probing methods, the path-probe is not triggered.

Note The path-probe technique makes a best effort to calculate the relative RTT for those D-proxies behind the firewall. This method involves tracing the path along with the RTT to all intermediate gateways between the probing device and the D-proxy. The calculated path information is then sent back to the querying GSS.

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 differs from the ICMP/TCP probe method by calculating RTT to the common gateway, not to the D-proxy.

9. In the Acceptable RTT field, enter a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. If the zones configured on the GSS report an RTT that is less than the specified Acceptable RTT value, the GSS does the following:

a. Disregards the acceptable percentage of zones.

b. Considers that there is sufficient proximity data to make a proximity decision.

c. Uses the zones reporting less than or equal to this value in the proximity decision.

Use this parameter to adjust the granularity of the proximity decision process. Enter an acceptable RTT value from 50 to 1500 ms. The default value is 100 ms.

10. 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. 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. Enter a percentage of zones from 3 to 100 percent. The default value is 40 percent.

Note If the reported RTT from one or more zones for the DNS rule/answer group is below the Acceptable RTT value, then the Acceptable Zone value is ignored by the GSS.

11. 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. In this case, the GSS proceeds to the next balance clause in the DNS rule.

The default setting is Disabled.

12. In the DRP Authentication drop-down list, enter the DRP authentication state:

    - **Enabled**—The GSS authenticates packets that it exchanges with the DRP agent in a probing device 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.

13. 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 (probing device) 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.

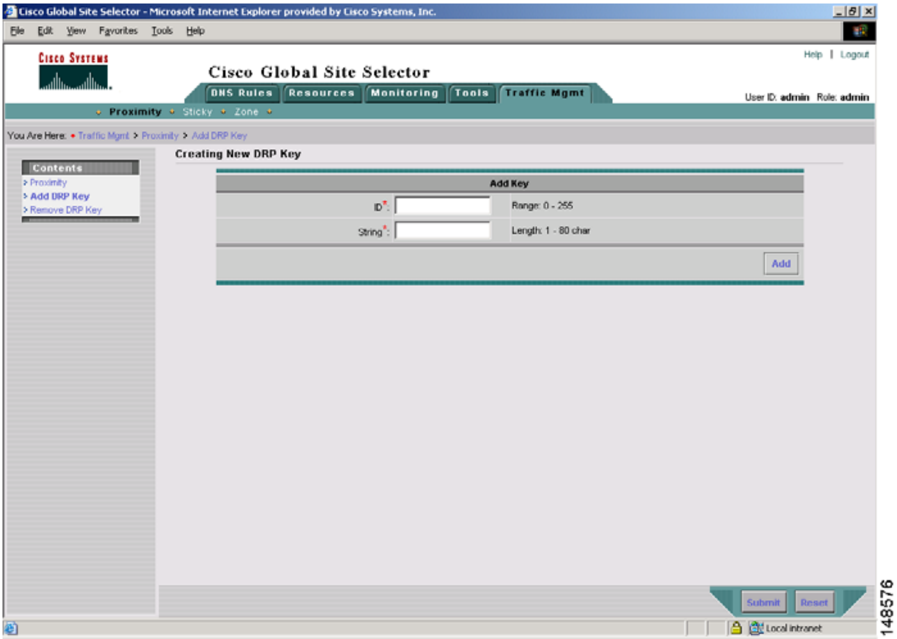
The DRP key is stored locally on each GSS in the network. The key functions as an encrypted password to help prevent DRP-based denial-of-service attacks, which can be a security threat. Each GSS generates DRP packets that contain all of the configured keys and sends the packets to the DRP agent in each configured zone. The DRP agent in each probing device examines the packet for a matching key (see the "Configuring the DRP Agent" section). If it finds a matching key, the DRP agent considers the DRP connection as authentic and accepts the packet.

To create a DRP authentication key:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (see Figure 9-10).

3. Click the **Add DRP Key** navigation link. The Creating New DRP Key details page appears (Figure 9-11).

Figure 9-11 Creating New DRP Key Details Page



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.
- **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.

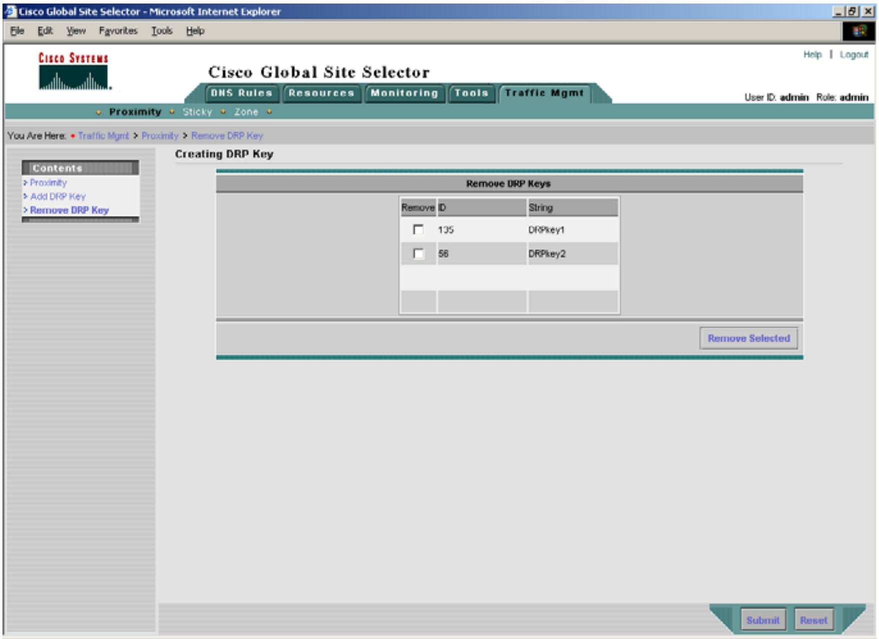
5. Click the **Add** button to create your DRP authentication key.
6. Click the **Submit** button to save your global proximity configuration changes.
7. Repeat this procedure to create additional DRP keys. The primary GSSM supports a maximum of 32 keys.

Deleting DRP Keys

To remove DRP authentication keys:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (see Figure 9-10).
3. Click the **Remove DRP Key** navigation link. The Remove DRP Key details page appears (Figure 9-12).

Figure 9-12 Remove DRP Key Details Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Proximity
Sticky
Zone
You Are Here: • Traffic Mgmt > Proximity > Remove DRP Key
Contents
Proximity
Add DRP Key
Remove DRP Key
Remove Selected
Submit
Reset
148651

Creating DRP Key

Remove DRP Keys

Remove	ID	String
□	135	DRPkey1
□	56	DRPkey2

4. Click the check box accompanying each DRP key that you want to remove from the list, 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 residing in GSS memory and sends that answer to the requesting D-proxy. If the PDB is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from probing devices in every zone in the proximity network, and puts the results in the PDB.

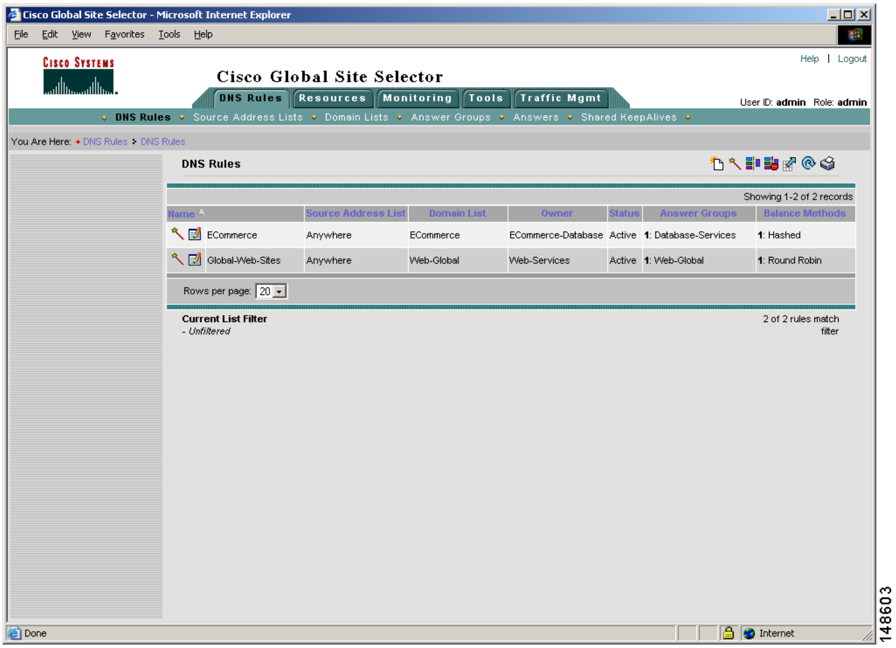
When there are no valid answers in the answer group of a proximity balance clause, the GSS skips that balance clause and moves on to the next clause listed in the DNS rule unless you specify a proximity Wait condition. In that case, the GSS waits to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client’s D-proxy until the GSS obtains sufficient proximity data to complete the selection process.

Note If you use DNS sticky and network proximity in your DNS rule, stickiness always takes precedence over proximity. When a valid sticky answer exists for a given DNS rule match, the GSS does not consider proximity when returning an answer to a client D-proxy.

To use the DNS Rule Builder to add proximity balance clauses to a DNS rule:

1. From the primary GSSM GUI, click the **DNS Rules** tab, then click the **DNS Rules** navigation link. The DNS Rules list page appears (Figure 9-13).

Figure 9-13 DNS Rules List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > DNS Rules
DNS Rules
Done
Internet
148603

Showing 1-2 of 2 records

Name	Source Address List	Domain List	Owner	Status	Answer Groups	Balance Methods
ECommerce	Anywhere	ECommerce	ECommerce-Database	Active	1: Database-Services	1: Hashed
Global-Web-Sites	Anywhere	Web-Global	Web-Services	Active	1: Web-Global	1: Round Robin

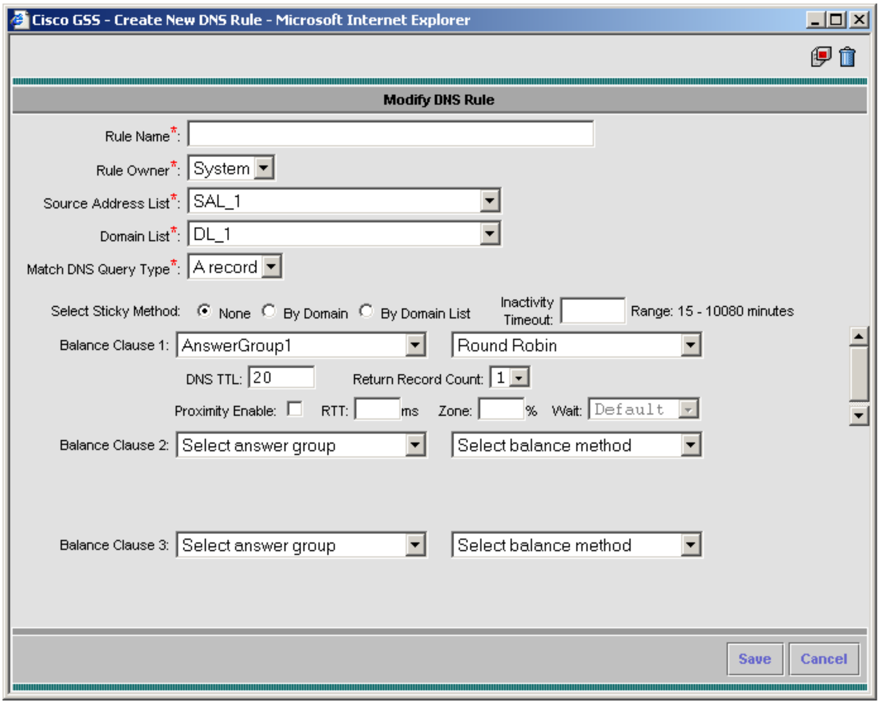
Rows per page: 20

Current List Filter
- *Unfiltered*

2 of 2 rules match filter

2. Click the **Open Rule Builder** icon. The Create New DNS Rule page opens in a separate window (Figure 9-14).

Figure 9-14 Create New DNS Rule Window



Cisco GSS - Create New DNS Rule - Microsoft Internet Explorer

Modify DNS Rule

Rule Name*:

Rule Owner*: System

Source Address List*: SAL_1

Domain List*: DL_1

Match DNS Query Type*: A record

Select Sticky Method: ● None ○ By Domain ○ By Domain List Inactivity Timeout: Range: 15 - 10080 minutes

Balance Clause 1: AnswerGroup1 Round Robin

DNS TTL: 20 Return Record Count: 1

Proximity Enable: □ RTT: ms Zone: % Wait: Default

Balance Clause 2: Select answer group Select balance method

Balance Clause 3: Select answer group Select balance method

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:
    - Select 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.
    - Select 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. 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.

      Enter an acceptable RTT value from 50 to 1500 ms. 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. 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 criterion. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

  Enter a percentage of zones from 3 to 100 percent. 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:

  –**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. In this case, the GSS proceeds to the next balance clause in the DNS rule.

6. Repeat steps 4 and 5 to select 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 operation 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 includes the following procedures:

- Logging in to the CLI and Enabling Privileged EXEC Mode
- Creating Proximity Groups
- Configuring Static Proximity Database Entries
- 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. Refer to 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:

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 (Global Site Selector or Global Site Selector Manager) through Telnet or SSH, enter the host name or IP address of the GSS to access the CLI.

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

For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, refer to 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>
```

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

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

Creating Proximity Groups

This section includes 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 ease of proximity group creation through automation scripts. The primary GSSM supports a maximum of 5000 proximity groups. Each proximity group contains one to 30 blocks of IP addresses and subnet masks (in dotted-decimal format).

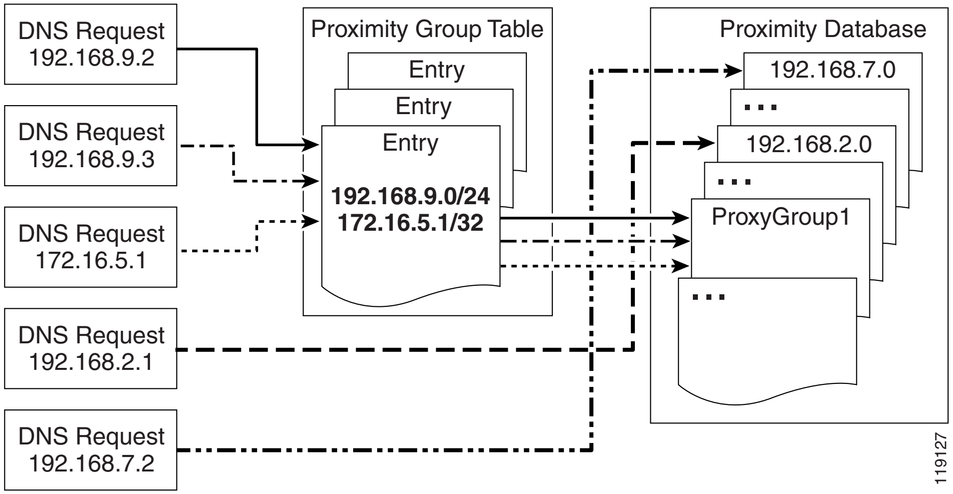
The benefits of proximity grouping include the following:

- Less probing activities performed by the GSS. 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. This reduces the overhead associated with probing.
- Less space required for the PDB. Instead of multiple PDB entries, the GSS uses only one entry for multiple D-proxies.
- User 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 9-15 illustrates how through proximity group entries 192.168.9.0/24 and 172.16.5.1/32, 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*. If no match is found in the PDB for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 9-15 Locating a Grouped Proximity Database Entry



Creating a Proximity Group

To create a proximity group, use the **proximity group** global server load-balancing configuration mode command from the primary GSSM CLI 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 ease of proximity group creation through automation 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:

proximity group {*groupname*} **ip** {*ip-address*} **netmas**k {*netmask*}

The options and variables are:

- *groupname*—Enter a unique alphanumeric name for the proximity group with a maximum of 80 characters. Use only alphanumeric characters and the underscore ("_") character.
- **ip** *ip-address*—The IP address block specified in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmas*k—The subnet mask of the IP address block, specified 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

To delete a previously configured IP address block from a proximity group, use the **no** form of the **proximity group** command. For example:

```
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

To delete a proximity group and all configured IP address blocks, use the **no** form of the **proximity group** command. For example:

```
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 includes the following procedures:

- Adding Static Proximity Entries
- Deleting Static Entries from the Proximity Database

Adding Static Proximity Entries

Entries in the PDB 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 find that you need to configure static proximity metrics for zones in your GSS network or to assign probing devices to specific D-proxies, define a series of static entries in the PDB by using the **proximity assign** global server load-balancing configuration mode command. If the same entry, dynamic or static, already exists in the proximity database, the GSS will overwrite that entry with the newly assigned entry. You can use automation scripts if you intend to add numerous static entries in the PDB of each GSS.

Note The **proximity assign** CLI command affects only the local GSS. If you want to add the same static entries in the PDB of the other GSS devices in your network, enter the **proximity assign** command at CLI of each GSS.

Static entries in the PDB do not age out and remain in the PDB until you delete them. In addition, static entries are not subject to the automatic database cleanup of least recently used entries when the PDB size is almost at the maximum number of entries. Use the **no** 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 probing devices to obtain RTT data. The GSS probes the alternative probe target for requests from D-proxies matching these static entries.

Static entries in the PDB are either static RTT-filled or probe-target IP-filled.

To create static entries in the PDB, use the **proximity assign** global server load-balancing configuration mode command. The syntax for this command is:

> **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 options and variable are:

- **group** *groupname*—Enter 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*—The D-proxy IP address entry to be created in the PDB.
- **probe-target** *ip-address*—(Optional) An alternate IP address to probe by the probing device. Normally, the probing device transmits a probe to the requesting D-proxy IP address to calculate RTT. If you find that the D-proxy cannot be probed from the probing device, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.
- **zone-data** "*zoneId:RTT*"—(Optional) The calculated RTT value for a zone, specified in "*zoneId:RTT*" format. For example, enter `"1:100"` to specify zone 3 with an RTT of 100 seconds. Valid entries for *zoneID* are 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 (one day). To specify multiple static *zone:RTT* pairs in the proximity group, separate each entry within the quotation marks by a comma, but without spaces between the entries (for example, "3:450,22:3890,31:1000").

This example shows how to configure an alternative probing target for the proximity group *ISP1*:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP1
probe-target 192.168.2.2
```

This example shows how to configure an alternative probing target for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0):

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign ip 192.168.8.0
probe-target 192.168.2.2
```

This example shows how to configure static RTT metrics for the proximity group ISP2 using zone indexes created previously through the primary GSSM 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. This command, however, does not delete PDB entries saved as part of an automatic dump to a backup file on disk, which the GSS loads upon a reboot or restart to initialize the PDB. To ensure that you successfully remove the desired PDB entries from both GSS memory and disk, enter the **proximity database delete** command followed by the **proximity database periodic-backup now** command to force an immediate backup of the empty PDB residing in GSS memory.

The syntax for this command is:

proximity database delete {**all** | **assigned** | **group** {*name*} | **inactive** *minutes* | **ip** {*ip-address*} **netmask** {*netmask*} | **no-rtt** | **probed**}

The options and variables are

- **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.

Caution Use the **proximity database delete all** command only when you want to remove all entries from the PDB to have an empty database. Ensure that you want to permanently delete entries from the PDB before you enter this command. You cannot retrieve PDB entries once they are deleted.

- **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:

```
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.

If desired, 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. Refer to the *Cisco Global Site Selector Administration Guide* for details about displaying the contents of a file.

The GSS includes a number of options to provide a level of granularity for dumping entries from the PDB. The GSS supports binary and Extensible Markup Language (XML) output formats. Optionally, you can specify filters, such as PDB entry type and entry IP network address, to clarify the information dumped from the PDB. PDB entry types can be either statically entered (see the "Configuring Static Proximity Database Entries" section) or dynamically learned by the GSS. You can instruct the GSS to dump both type of entries from the PDB. If you do not specify an entry type, the GSS automatically dumps all entries from the PDB.

If you attempt to overwrite an existing proximity database dump file with the same filename, the GSS displays the following message: `Proximity Database dump failed, a file with that name already exists.`

To dump entries contained in the PDB to a named file, use the **proximity database dump** command.

The syntax for this command is:

> **proximity database dump** {*filename*} **format** {**binary** | **xml**} [**entry-type** {**all** | **assigned** | **probed**}] [**entry-address** {*ip-address*} **netmask** {*netmask*}]

The options and variables are:

- *filename*—The name of the output file containing the PDB entries on the GSS disk. This file resides in the /home directory.
- **format**—Dumps the PDB entries in binary or XML format. Select 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:
  - **binary**—Dumps the assigned proximity entries in true binary format. This file can only be used 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 two to four 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:
  - **all**—Dump static and dynamic entries from the PDB
  - **assigned**—Dump statically assigned proximity entries
  - **probed**—Dump dynamically probed proximity entries

  The default is **all**.
- **entry-address** *ip-address*—The IP address of the PDB entry.
- **netmask** *netmask*—The subnet mask of the PDB entry in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to dump the dynamic PDB entries to a file named *PDB2004_6_30* in XML format. If the dump is large, progress messages appear.

```
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 time.

The syntax for this command is:

proximity database periodic-backup now

For example, enter:

```
gss1.example.com# proximity database periodic backup now
```

Loading Proximity Database Entries

The GSS supports the loading and merging of 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 non-overlapping database entries.

To load a PDB from disk into GSS memory, use the **proximity database load** command. The syntax for this command is:

proximity database load *filename* **format binary** [**override**]

The options and variable are:

- *filename*—Specifies 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 select 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:
  - 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.

There may be instances when you need to instruct the probing device in one or all zones (broadcast) to send a probe to a specific D-proxy address, obtain an RTT value, and save the entry in the PDB. To initiate direct probing to a specific D-proxy IP address or direct probing to one or more zones, use the **proximity probe** command.

The syntax for this command is:

proximity probe {*dproxy_address*} [**zone** {*zoneId* | **all**}]

The options and variables are:

- *dproxy_address*—The IP network address of the D-proxy that you want to probe from the probing device.
- **zone** *zoneId*—The ID of the proximity zone containing the probing device from which you want to initiate a probe. Available values are from 1 to 32.
- **all**—The GSS instructs the probing devices in all configured zones to transmit a probe to the specified D-proxy IP address.

For example, to instruct the probing device in zone 1 to send a probe to the D-proxy at 172.16.5.7, enter:

```
gss1.example.com# proximity probe 172.16.5.7 zone 1
```

Disabling Proximity Locally on a GSS for Troubleshooting

You can disable proximity for a single GSS when you need to locally override the 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
```

CHAPTER 10

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, the **show statistics dns** command can be used 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 sections 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 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 content routing agents (CRAs), to determine which server is best able to respond to a given request. 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 for the **show statistics boomerang** command is:

show statistics boomerang {domain *domain_name* | **global}**

The options and variables are:

- **domain**—Displays statistics related to a named domain being served by the GSS.
- *domain_name*—Specifies the name of the domain.
- **global**—Displays statistics across the entire GSS network for the Boomerang server.

This example shows how to displays statistics across the entire GSS network for the boomerang server:

```
gss1.yourdomain.com# show statistics boomerang global
Boomerang global statistics:
        Total races: 24
```

This example shows how to displays boomerang statistics for a specific domain:

```
gss1.yourdomain.com# show statistics boomerang domain1
Domain statistics: (of domain1)
        DNS A requests:
```

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. 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 procedures:

- Displaying Answer Statistics
- Displaying Answer Group Statistics
- Displaying Domain Statistics
- Displaying Domain List Statistics
- Displaying Global Statistics
- Displaying DNS Rule Proximity Statistics
- Displaying DNS Rule Statistics
- Displaying Source Address Statistics
- Displaying Source Address List Statistics
- Displaying DNS Rule Sticky Statistics

Displaying Answer Statistics

Use the **show statistics dns answer** command to display the accumulated hit count for each configured answer that responds to content queries. The statistics also include the per second average hit count calculated during the last-minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is:

show statistics dns answer {**list** | *answer_name*}

The options and variables are:

- **list**—Lists the names of all answers configured for the GSS.
- *answer_name*—Specifies the name of the answer that you want to view statistics.

Table 10-1 describes the fields in the **show statistics dns answer** command output.

Table 10-1 Field Descriptions for show statistics dns answer Command

Field	Description
Answer	Name of the answer. Depending on the type of answer, the GSS displays: • The VIP address of the answer (VIP-type answer) • Interface or circuit address (CRA-type answer) • The 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.

Table 10-1 Field Descriptions for show statistics dns answer Command (continued)

Field	Description
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 Group Statistics

Use the **show statistics dns answer-group** command to display the total hit count for each configured answer group and the answers contained in the answer group.

The syntax for the command is:

show statistics dns answer-group {**list** | *group_name* [**verbose**]}

The options and variables are:

- **list**—Lists the names of all answer groups configured for the GSS.
- *group_name*—Specifies the 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 10-2 describes the fields in the **show statistics dns answer-group verbose** command output.

Table 10-2 Field Descriptions for show statistics dns answer-group verbose Command

Field	Description
Total Hit Count	Accumulated hit count for the configured answer group since the GSS was last started.
Answer	Name of each answer in the answer group. Depending on the type of answer, the GSS displays: • The VIP address of the answer (VIP-type answer) • Interface or circuit address (CRA-type answer) • The IP address of the name server (Name Server-type answer)
Hit Count	Number of times the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.
Status	Indicates whether the answer is online (up) or offline (down).

Displaying Domain Statistics

Use the **show statistics dns domain** command to display the accumulated hit count for each configured host domain. The statistics also include the per-second average hit count calculated during the last minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is:

show statistics dns domain {**list** | *domain_name*}

The options and variables are:

- **list**—Lists the names of all domains configured for the GSS.
- *domain_name*—Specifies the name of the domain that you want to view statistics.

Table 10-3 describes the fields in the **show statistics dns domain** command output.

Table 10-3 Field Descriptions for show statistics dns domain Command

Field	Description
Domain	Name of the hosted domain
Total Hits	Total number of hits for the specified hosted domain since the GSS was last started
1-Min	Averaged per second hit count for the hosted domain, calculated during the last minute
5-Min	Averaged per second hit count for the hosted domain, calculated during the last 5-minute interval
30-Min	Averaged per second hit count for the hosted domain, calculated during the last 30-minute interval
4-Hr	Averaged per second hit count for the hosted domain, calculated during the last 4-hour interval

Displaying Domain List Statistics

Use the **show statistics dns domain-list** command to display the total accumulated hit count for each configured domain list.

The syntax for the command is:

show statistics dns domain-list {**list** | *domain_list_name* [**verbose**]}

The options and variables are:

- **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 10-4 describes the fields in the **show statistics dns domain-list verbose** command output.

Table 10-4 Field Descriptions for show statistics dns domain-list verbose Command

Field	Description
Total Hit Count	Accumulated hit count for the hosted domain since the GSS was last started or statistics cleared
Domain Name	Name of the hosted domain in the domain list
Hit Count	Number of times the hosted domain has been selected or matched in the DNS rule when the GSS processes a DNS request

Displaying Global Statistics

Use the **show statistics dns global** command to display general DNS statistics for the GSS device in use.

The syntax for the command is:

show statistics dns global

Table 10-5 describes the fields in the **show statistics dns global** command output.

Table 10-5 Field Descriptions for show statistics dns global Command

Field	Description
DnsQueriesRcvd	Total number of DNS queries received by the GSS from a requesting client D-proxy
DnsHostAddrQueriesRcvd	Total number of host address queries received by the GSS from a requesting client D-proxy
DnsResponsesSent	Total number of DNS responses sent by the GSS to a requesting client D-proxy
DnsResponsesNoError	Total number of DNS responses sent by the GSS to a requesting client D-proxy without an error
DnsResponsesErrors	Total number of DNS responses sent by the GSS to a requesting client D-proxy with an error
DnsServfailRCode	DNS server failure return code
DnsNxdomainRCode	DNS NX domain return code
DnsNotimpRCode	DNS not implemented return code
DnsRefusedRCode	DNS refused return code
DnsQueriesUnmatched	Total number of unmatched DNS queries received by the GSS from a requesting client D-proxy
DnsDrops	Total number of DNS queries dropped by the GSS
DnsNSFWDSent	Total number of queries that do not match domains on any GSS domain lists and have been forwarded by the GSS to an external DNS name server for resolution

Table 10-5 Field Descriptions for show statistics dns global Command (continued)

Field	Description
DnsBoomServReqSent	Total number of requests sent by the boomerang server in the GSS to initiate a DNS race
DnsNSFWDResponsesRcvd	Total number of queries that have been forwarded to the GSS to an external DNS name server for resolution
DnsProxLkupReqSent	Total number of proximity lookup requests sent by the selector to the proximity subsystem
DnsProxLkupRespRecd	Total number of proximity lookup requests received by the selector from the proximity subsystem
DnsReqRatePerSecondCur	Current request rate per second that requests are made to the GSS to perform a DNS resolution
DnsReqRatePerSecondPeak	Peak request rate per second that requests are made to the GSS to perform a DNS resolution
DnsStickyLkupReqSent	Total number of sticky lookup requests sent by the selector to the sticky subsystem
DnsStickyAddReqSent	Total number of requests for IP addresses sent by the selector to the sticky subsystem
DnsStickyHit	Total number of successful sticky answer matches for the DNS rule
DnsStickyMiss	Total number of times the GSS was unable to provide the sticky answer for the DNS rule
DnsSrcPortErrorUdp	Total number of UDP errors that occurred on the DNS source port
DnsSrcPortErrorTcp	Total number of TCP errors that occurred on the DNS source port
DnsPollSocketError	Total number of socket connection errors

Displaying DNS Rule Proximity Statistics

Use the **show statistics dns proximity rule** command to display all proximity lookups by DNS rule name.

Note To clear proximity statistics related to the DNS server component of the GSS, use the **clear statistics dns** command. See the "Clearing GSS Global Server Load-Balancing Statistics" section for details.

The syntax for the command is:

show statistics dns proximity rule

Table 10-6 describes the fields in the **show statistics dns proximity rule** command output.

Table 10-6 Field Descriptions for show statistics dns proximity rule Command

Field	Description
Rule	Name of the matched DNS rule
Proximity Hit Count	Number of DNS requests that match the DNS rule
Proximity Success Count	Number of DNS responses successfully returned with a proximate answer for the DNS rule

Displaying DNS Rule Statistics

Use the **show statistics dns rule** command to display the total hit count and success count for each configured DNS rule.

The syntax for the command is:

show statistics dns rule {**list** | *rule_name*}

The options and variables are:

- **list**—Lists the names of all DNS rules configured for the GSS.
- *rule_name*—Specifies the name of the DNS rule that you want to view statistics.

Table 10-7 describes the fields in the **show statistics dns rule** command output.

Table 10-7 Field Descriptions for show statistics dns rule Command

Field	Description
Total Hit Count	Accumulated hit count for the configured DNS rule since the GSS was last started.
Total Success Count	Accumulated number of successful answer matches for the DNS rule.
Clause	Number of the balance clause in the DNS rule.
Hit Count	Number of times the DNS rule processed a DNS request.
Success Count	Number of successful answer matches for the DNS rule.
Id	Internal ID number of the answer in the DNS rule.
Address	Name of the answer. Depending on the type of answer, the GSS displays: • The VIP address of the answer (VIP-type answer) • Interface or circuit address (CRA-type answer) • The IP address of the name server (Name Server-type answer)
Hit Count	Number of times the answer has been selected or matched in the DNS rule when the GSS processes a DNS request.

Displaying Source Address Statistics

Use the **show statistics dns source-address** command to display the accumulated hit count for each configured source address. The statistics also includes the per-second average hit count calculated during the last-minute, a 5-minute interval, a 30-minute interval, and a 4-hour interval.

The syntax for the command is:

show statistics dns source-address {**list** | *sa_name*}

The options and variables are:

- **list**—Lists the names of all source addresses configured for the GSS.
- *sa_name*—Specifies the name of the source address that you want to view statistics.

Table 10-8 describes the fields in the **show statistics dns source-address** command output.

Table 10-8 Field Descriptions for show statistics dns source-address Command

Field	Description
Src Address	IP address or CIDR address block of the client DNS proxy
Total Hits	Total number of hits for the source address since the GSS was last started or statistics cleared
1-Min	Averaged per second hit count for the source address, calculated during the last minute
5-Min	Averaged per second hit count for the source address, calculated during the last 5-minute interval
30-Min	Averaged per second hit count for the source address, calculated during the last 30-minute interval
4-Hr	Averaged per second hit count for the source address, calculated during the last 4-hour interval

Displaying Source Address List Statistics

Use the **show statistics dns source-address-list** command to display the total hit count for each configured source address list. The statistics also include the last minute average, 5-minute average, 30-minute average, and 4-hour average of the hit counts.

The syntax for the command is:

show statistics dns source-address-list {**list** | *sa_list_name* [**verbose**]}

The options and variables are:

- **list**—Lists the names of all source addresses.
- *sa_list_name*—Specifies the 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 10-9 describes the fields in the **show statistics dns source-address-list** command output.

Table 10-9 Field Descriptions for show statistics dns source-address-list verbose Command

Field	Description
Total Hit Count	Accumulated hit count for the configured source address list since the GSS was last started or statistics cleared
Source Address	IP address or CIDR address block of the client DNS proxy
Hit Count	Number of times the source address has been selected or matched in the DNS rule when the GSS processes a DNS request

Displaying DNS Rule Sticky Statistics

Use the **show statistics dns sticky rule** command to display all DNS sticky lookups by DNS rule name.

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 for the command is:

show statistics dns sticky rule

Table 10-10 describes the fields in the **show statistics dns sticky rule** command output.

Table 10-10 Field Descriptions for show statistics dns sticky rule Command

Field	Description
Rule	Name of the matched DNS rule
Sticky Hit Count	Total number of lookups in the sticky database for the DNS rule
Sticky Success Count	Total number of successful sticky answer matches for the DNS rule

Monitoring the Status of the DRP Agent on a GSS

Use the **show statistics drpagent** command to monitor statistics on the Director Response Protocol (DRP) agent.

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 for the command is:

show statistics drpagent

Table 10-11 describes the fields in the **show statistics drpagent** command output.

Table 10-11 Field Descriptions for show statistics drpagent Command

Field	Description
DRP agent enabled/disabled	Indicates whether the DRP agent is enabled or disabled.
director requests	Number of director requests.
successful measured lookups	Number of successful DRP measure requests received by the DRP agent from all of the GSSs.
packet failures returned	Number of packet failures returned.
successful echos	Number of successful DRP echo requests (DRP keepalives) received by the DRP agent from all of the GSSs.
path-rtt probe source port	Source port of the path probe packets from the DRP agent.
path-rtt probe destination port	Destination port of the path probe packets from the DRP agent.
tcp-rtt probe source port	Source port of the TCP probe packets from the DRP agent.
tcp-rtt probe destination port	Destination port of the TCP probe packets from the DRP agent.

Monitoring DDoS Statistics on a GSS

This section describes the procedures you need to follow to display DDoS statistics from the CLI and includes the following:

- Displaying DDoS Attack Statistics
- Displaying DDoS Anti-Spoofing Statistics
- Displaying DDoS Failed DNS Queries

- Displaying DDoS Rate-Limit Values
- Displaying DDoS Running Configuration
- Displaying DDoS Statistics
- Displaying DDoS Status

Displaying DDoS Attack Statistics

Use **show ddos attacks** (from privileged EXEC mode) or **show attacks** (from ddos configuration mode) to show the DNS attacks detected by the GSS.

Note Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is:

show [**ddos**] **attacks**

Table 10-12 describes the fields in the **show** [**ddos] attacks** command output.

Table 10-12 Field Descriptions for show [*ddos*] *attacks Command*

Field	Description
Total Attacks	Total number of DNS attacks detected by the GSS.
Reflection attack	An 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.
Malformed DNS packet attacks	An attack in which the GSS is flooded with malformed DNS packets.
Failed Global Domain attacks	The failed domain counter provides a total for DNS queries that failed to match the global domain name.
Global Rate-limit exceeded attacks	An attack in which the maximum number of DNS requests the GSS receives from the D-proxy per second exceeds the global limit.

For example:

```
gssm1.example.com(config-ddos)# show attacks

    Total Attacks                     :0
        Reflection attack                 :0
        Malformed DNS packet attacks      :0
        Failed Global Domain attacks      :0
        Global Rate-limit exceeded attacks:0
```

Displaying DDoS Anti-Spoofing Statistics

Use **show ddos dproxy** (from privileged EXEC mode) or **show dproxy** (from ddos configuration mode) to show the spoofed and trusted D-proxies on the GSS.

Note Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is:

show [**ddos**] **dproxy** [*ipaddress* | **spoofed** | **trusted**]

The options and variables are:

- *ipaddress*—Specifies the D-proxy IP address.
- **spoofed**—Shows the spoofed D-proxies.
- **trusted**—Shows the trusted D-proxies.

Table 10-13 describes the fields in the **show** [**ddos**] **dproxy** command output.

Table 10-13 Field Descriptions for show [ddos] d-proxy Command

Field	Description
Dproxy Address	IP address of the D-proxy.
Spoofed/Nonspoofed	Spoofed or non-spoofed D-proxy.
Drops	Number of dropped packets due to anti-spoofing failure.

For example:

```
gssm1.example.com# show ddos dproxy 16.1.1.11

    DPROXY ADDRESS     SPOOFED/NONSPOOFEDDROPS
    ----------         ------              ---------------
    16.1.1.11          Spoofed             3
```

Displaying DDoS Failed DNS Queries

Use **show ddos failed-dns** (from privileged EXEC mode) or **show failed-dns** (from ddos configuration mode) to show:

- the last *x* number of domain names that caused failed DNS queries at the GSS
- the number of failed DNS queries per D-proxy

Failed DNS queries refer to DNS queries for a domain not configured on the GSS.

Note Before enabling the ddos configuration mode, ensure that the DDoS license has already been installed on the GSS. For more details, see the *Cisco Global Site Selector Administration Guide*.

The syntax for the command is:

show [**ddos**] **failed-dns** [**failed-domains** | **global-domain-rules** | **gslb-rules**]

The options and variables are:

- **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 10-14 describes the fields in the **show** [**ddos**] **failed-dns** command output.

Table 10-14 Field Description for show [*ddos*] *failed-dns Command*

Field	Description
Global domain check drops	Number of dropped packets as a result of a global domain name check.
Dproxy Address	IP address of the D-proxy.
Number of Failed DNS queries	Number of failed DNS queries as a result of a GSLB-rule check.

For example:

```
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

Use **show ddos rate-limit** (from privileged EXEC mode) or **show rate-limit** (from ddos configuration mode**)** to show the rate-limits per D-proxy and the number of packets dropped per source.

The syntax for the command is:

show [**ddos**] **rate-limit** [*ipaddress* | **global** | **unknown**]

The options and variables are:

- *ipaddress*—Specifies the 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 10-15 describes the fields in the **show** [**ddos] rate-limit** command output.

Table 10-15 Field Descriptions for show* [*ddos*] *rate-limit Command

Field	Description
Dproxy Address	IP address of the D-proxy.
Rate-limit	Maximum number of DNS requests the GSS can receive from a D-proxy per second.
Applied Rate Limit	This value is based on the following: rate-limit * scaling factor/100
Drops	Number of packets dropped because of the rate-limit.

For example:

```
gssm1.example.com# show ddos rate-limit 16.1.1.11

    Dproxy Address      Rate-limit  Applied Rate Limit     Drops
    ----------          ------      ---------------        -----
    16.1.1.11           0           12000                  0
```

Displaying DDoS Running Configuration

Use **show ddos-config** (from privileged EXEC or ddos configuration mode) to display the contents of the DDos running configuration file.

The syntax for the command is:

show ddos-config

Table 10-16 describes the fields in the **show ddos-config** command output.

Table 10-16 Field Descriptions for show ddos-config Command

Field	Description
enable	DDoS detection and mitigation module status, enabled or disabled.
rate-limit global	Global rate-limit configured on the GSS.

Table 10-16 Field Descriptions for show ddos-config Command

Field	Description
tolerance factor	Helps determine the rate-limit.
peacetime database	Peacetime database identifier.
global domain	Global domain name identifier.
dproxy trusted	A D-proxy added or deleted from a trusted D-proxy database.
mitigation-rule response enable	Enables mitigation rules for the following DNS responses: • Packets are dropped with a source port other than 53 and QR bit of 1 (response) when responses come from a source port other than 53. • Packets are dropped with a destination port of 53 and a QR bit of 1 (response) when responses come to port 53.
mitigation-rule request enable	Enables mitigation rules for DNS requests in which packets are dropped with a source port equal to 53, but less than 1024, and a QR bit of 0 (request).

For example:

```
gssm1.example.com# show ddos running-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

Use **show statistics ddos** (from privileged EXEC mode)**,** or **show statistics** (from ddos configuration mode) to display DDoS statistics.

Note To clear statistics related to the DDoS detection and mitigation component of the GSS, use the **clear statistics ddos** command. See the "Clearing GSS Global Server Load-Balancing Statistics" section for details.

The syntax for the command is:

show statistics [**ddos**] [**attacks** | **global**]

The options and variables are:

- **attacks**—Displays attack statistics.
- **global**—Displays global statistics.

Table 10-17 describes the fields in the **show statistics ddos attacks** command output.

Table 10-17 Field Descriptions for show statistics ddos attacks Command

Field	Description
Total Attacks	Total number of DDoS attacks on the GSS.
Reflection attacks	An 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
Malformed DNS packet attacks	An attack in which the GSS is flooded with malformed DNS packets.
Failed Global Domain attacks	An attack in which the GSS is flooded with failed global domain attacks.
Global Rate-limit exceeded attacks	An attack in which the global rate-limit threshold has been exceeded.

For example:

```
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 10-18 describes the fields in the **show statistics ddos global** command output.

Table 10-18 Field Descriptions for show ddos statistics global Command

Field	Description
Total packets received	Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.
Total packets dropped	Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.
Total Anti-spoofing triggered	Total number of packets that triggered the GSS anti-spoofing mechanism.
Total Validated DNS requests	Total number of packets successfully identified as part of an anti-spoofing attack.
Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation rate-limiting functions as part of an attack and dropped. The rate limit is the maximum number of DNS requests the GSS can receive from the D-proxy per second.
Global Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.
Unknown dproxies drops	An D-proxy that has not been classified as spoofed or non-spoofed by the DDoS protection and mitigation function is unknown. The DDoS function starts anti-spoofing for an unknown D-proxy. If the number of packets from unknown D-Proxies exceeds the specified rate limit, the unknown drops start.

Table 10-18 Field Descriptions for show ddos statistics global Command

Field	Description
Spoofed packet drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an attack and dropped.
Malformed packet drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a malformed packet and dropped.
Mitigation rules drops	Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.
Global domain name drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.
Ongoing anti-spoofing drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.

For example:

```
gssm1.example.com# show statistics ddos global
    Total packets received    :6
    Total packets dropped     :2

    Total Anti-Spoofing triggered :0
    Total Validated DNS requests  :0

    Dropped Packets Statistics:
    -----------------------------
    Rate limit drops              :0
    Global Rate limit drops       :0
    Unknown dproxies drops        :0
    Spoofed packet drops          :2
    Malformed packet drops        :0
    Mitigation rule drops         :0
    Global domain drops           :0
    Ongoing anti-spoofing drops   :0
```

Displaying DDoS Status

Use **show ddos status** (from privileged EXEC mode) or **show status** (from ddos configuration mode) to display DDoS statistics.

The syntax for the command is:

show [**ddos**] **status**

Table 10-19 describes the fields in the **show ddos status** command output.

Table 10-19 Field Description for show [*ddos*] *status Command*

Field	Description
DDoS Status	Status of the DDoS detection and mitigation module in the GSS, either enabled or disabled.

For example:

```
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.

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 procedures:

- Displaying CRA Keepalive Statistics
- Displaying Global Keepalive Statistics
- Displaying HTTP HEAD Keepalive Statistics
- Displaying ICMP Keepalive Statistics
- Displaying KAL-AP Keepalive Statistics
- Displaying Scripted Keepalive Statistics

- Displaying Scripted Keepalive Statistics
- Displaying TCP Keepalive Statistics

Displaying CRA Keepalive Statistics

Use the **show statistics keepalive cra** command to display statistics for configured content routing agent (CRA) keepalive types managed by the GSS and used with boomerang-type answers.

The syntax for the command is:

show statistics keepalive cra {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured CRA-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-20 describes the fields in the **show statistics keepalive cra all** command output.

Table 10-20 Field Descriptions for show statistics keepalive cra all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	Name assigned to the answer.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
One Way Delay	One-way delay time, in milliseconds, used by the GSS to calculate a static round-trip time (RTT), with the one-way delay constituting one-half of the round-trip time that is used for all DNS races involving this answer.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.

Table 10-20 Field Descriptions for show statistics keepalive cra all Command

Field	Description
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying Global Keepalive Statistics

Use the **show statistics keepalive global** command to display all keepalive statistics managed by the GSS device.

The syntax for the command is:

show statistics keepalive global

Table 10-21 describes the fields in the **show statistics keepalive global** command output.

Table 10-21 Field Descriptions for show statistics keepalive global Command

Field	Description
ICMP Probe Success Count	Number of ICMP queries sent to the answer that resulted in a successful response
ICMP Probe Failure Count	Number of ICMP queries sent to the answer that resulted in a failure
ICMP 'echo request' packets sent	Number of ICMP echo request messages sent to the answer
ICMP 'echo reply' packets received	Number of ICMP echo reply messages received by the GSS from the answer

Table 10-21 Field Descriptions for show statistics keepalive global Command (continued)

Field	Description
Configured ICMP Probe Count	Number of configured ICMP probes sent to the answer
ONLINE ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Online state for the keepalive
OFFLINE ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Offline state for the keepalive
SUSPENDED ICMP Probe Count	Number of ICMP probes sent to the answer that returned a Suspended state for the keepalive
INIT ICMP Probe Count	Number of ICMP probes sent to the answer that returned an Init state for the keepalive
DNS Probe Success Count	Number of DNS request probes sent by the GSS that resulted in a successful response
DNS Probe Failure Count	Number of DNS request probes sent by the GSS that resulted in a failure
DNS packets sent	Number of DNS request packets sent by the GSS
DNS packets received	Number of DNS request packets received by the GSS
Configured DNS Probe Count	Number of DNS request probes sent by the GSS
ONLINE DNS Probe Count	Number of DNS request probes sent that returned an Online state for the keepalive
OFFLINE DNS Probe Count	Number of DNS request probes that returned an Offline state for the keepalive
SUSPENDED DNS Probe Count	Number of DNS request probes sent that returned a Suspended state for the keepalive
INIT DNS Probe Count	Number of DNS request probes sent that returned an Init state for the keepalive
KAL-AP Probe Success Count	Number of KAL-AP queries sent to the answer that resulted in a successful response
KAL-AP Probe Failure Count	Number of KAL-AP queries sent to the answer that resulted in a failure

Table 10-21 Field Descriptions for show statistics keepalive global Command (continued)

Field	Description
KAL-AP packets sent	Number of KAL-AP packets sent to the answer
KAL-AP packets received	Number of KAL-AP packets received by the GSS from the answer
Configured KAL-AP Probe Count	Number of configured KAL-AP probes sent to the answer
ONLINE KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Online state for the keepalive
OFFLINE KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive
SUSPENDED KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive
INIT KAL-AP Probe Count	Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive
CRA Probe Success Count	Number of CRA queries sent to the answer that resulted in a successful response
CRA Probe Failure Count	Number of CRA queries sent to the answer that resulted in a failure
CRA packets sent	Number of CRA packets sent to the answer
CRA packets received	Number of CRA packets received by the GSS from the answer
Configured CRA Probe Count	Number of configured CRA probes sent to the answer
ONLINE CRA Probe Count	Number of CRA probes sent to the answer that returned an Online state for the keepalive
OFFLINE CRA Probe Count	Number of KAL-AP probes sent to the answer that returned an Offline state for the keepalive
SUSPENDED CRA Probe Count	Number of KAL-AP probes sent to the answer that returned a Suspended state for the keepalive
INIT CRA Probe Count	Number of KAL-AP probes sent to the answer that returned an Init state for the keepalive

Table 10-21 Field Descriptions for show statistics keepalive global Command (continued)

Field	Description
HTTP-HEAD Probe Success Count	Number of HTTP-HEAD queries sent to the answer that resulted in a successful response
HTTP-HEAD Probe Failure Count	Number of HTTP-HEAD queries sent to the answer that resulted in a failure
HTTP-HEAD packets sent	Number of HTTP-HEAD packets sent to the answer
HTTP-HEAD packets received	Number of HTTP-HEAD packets received by the GSS from the answer
Configured HTTP-HEAD Probe Count	Number of configured HTTP-HEAD probes sent to the answer
ONLINE HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Online state for the keepalive
OFFLINE HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Offline state for the keepalive
SUSPENDED HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned a Suspended state for the keepalive
INIT HTTP-HEAD Probe Count	Number of HTTP-HEAD probes sent to the answer that returned an Init state for the keepalive
TCP Probe Success Count	Number of TCP queries sent to the answer that resulted in a successful response
TCP Probe Failure Count	Number of TCP queries sent to the answer that resulted in a failure
TCP packets sent	Number of TCP packets sent to the answer
TCP packets received	Number of TCP packets received by the GSS from the answer
Configured TCP Probe Count	Number of configured TCP probes sent to the answer

Table 10-21 Field Descriptions for show statistics keepalive global Command (continued)

Field	Description
ONLINE TCP Probe Count	Number of TCP probes sent to the answer that returned an Online state for the keepalive
OFFLINE TCP Probe Count	Number of TCP probes sent to the answer that returned an Offline state for the keepalive
SUSPENDED TCP Probe Count	Number of TCP probes sent to the answer that returned a Suspended state for the keepalive
INIT TCP Probe Count	Number of TCP probes sent to the answer that returned an Init state for the keepalive
Total Configured Probe Count	Total number of configured keepalive probes

Displaying HTTP HEAD Keepalive Statistics

Use the **show statistics keepalive http-head** command to display statistics for configured HTTP HEAD keepalive types managed by the GSS and used with VIP-type answers.

The syntax for the command is:

show statistics keepalive http-head {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured HTTP HEAD-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-22 describes the fields in the **show statistics keepalive http-head all** command output.

Table 10-22 Field Descriptions for show statistics keepalive http-head all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	The Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Destination Port	Port on the remote device receiving the HTTP HEAD-type keepalive request from the GSS.
HTTP Path	Default path that is relative to the server website being queried in the HTTP HEAD request.
Host Tag	Domain name that is sent to the VIP as part of the HTTP HEAD query in the Host tag field of the shared keepalive configuration.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying ICMP Keepalive Statistics

Use the **show statistics keepalive icmp** command to display statistics for configured ICMP keepalive types managed by the GSS and used with VIP-type answers.

The syntax for the command is:

show statistics keepalive icmp {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured ICMP-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-23 describes the fields in the **show statistics keepalive icmp all** command output.

Table 10-23 Field Descriptions for show statistics keepalive icmp all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	The Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.

Table 10-23 Field Descriptions for show statistics keepalive icmp all Command

Field	Description
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying KAL-AP Keepalive Statistics

Use the **show statistics keepalive kalap** command to display statistics for configured KAL-AP keepalive types managed by the GSS and used with VIP-type answers.

The syntax for the command is:

show statistics keepalive kalap {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured KAL-AP-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-24 describes the fields in the **show statistics keepalive kalap all** command output.

Table 10-24 Field Descriptions for show statistics keepalive kalap all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.

Table 10-24 Field Descriptions for show statistics keepalive kalap all Command (continued)

Field	Description
Keepalive Type	The Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Tag	Alphanumeric tag associated with the VIP in the KAL-AP request.
Primary Circuit	Primary (master) IP address.
Secondary Circuit	Secondary (backup) IP address.
Load	Load threshold value used to determine whether an answer is available, regardless of the balance method used.
Circuit Transitions	Number of times the circuit changed state.
VIP Failovers	Number of times the VIP switched to or from the primary DNS server and the secondary DNS server.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying Scripted Keepalive Statistics

Use the **show statistics keepalive scripted-kal** command to display statistics for configured Scripted keepalive types managed by the GSS and used with VIP-type answers.

The syntax for the command is:

show statistics keepalive scripted-kal {*name* | **all** | **list**}

The options and variables are:

- *name*—Specifies the KAL name for which you wish to display keepalive statistics.
- **all**—Displays all configured Scripted keepalives.
- **list**—Lists all available IP addresses.

Table 10-24 describes the fields in the **show statistics keepalive scripted-kal all** command output.

Table 10-25 Field Descriptions for show statistics keepalive scripted-kal all Command

Field	Description
IP	IP address of the SLB.
Keepalive	Target IP address of the keepalive.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Keepalive Type	Type of keepalive The potential types are CRA, ICMP, TCP, KAL-AP, Answer, Scripted keepalive, and HTTP-HEAD.
Kal Name	Name of the applicable keepalive.
Scripted Kal Type	Type of Scripted keepalive. The potential types are cisco-slb, f5-slb, snmp-mib-indexed-by-vip, snmp-mib-not-indexed-by-vip, and snmp-scalar.

Table 10-25 Field Descriptions for show statistics keepalive scripted-kal all Command (continued)

Field	Description
OID	SNMP request sent for this OID.There are two types of OIDs: scalar and vector or table. For a scalar-type OID, the filter is not required, while for a vector-type, it is a must. When you query for the vector OID, you get all the information in the table describing all of the VIPs configured at the target device. In this data, the load information for some VIPs configured at the GSS is the only information of real value, however.
Community Name	SNMP community name defined at the target device.
Filter	Required entry when fetching load information for some VIPs configured at the GSS.
Load	Load threshold value used to determine whether an answer is available, regardless of the balance method used.
Max VIP Load	Value the user sets at the Answer page.
No. of Execution	Number of times the script is executed.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
VIP GID	VIP Global ID number used by the GSS.
LID	Local ID number used by the GSS.
Keepalive GID	Global ID number of the keepalive.

Displaying Name Server Keepalive Statistics

Use the **show statistics keepalive ns** command to display statistics for configured name server (NS) keepalive types managed by the GSS and used with name server type answers.

The syntax for the command is:

show statistics keepalive ns {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured name server-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-27 describes the fields in the **show statistics keepalive ns all** command output.

Table 10-26 Field Descriptions for show statistics keepalive ns all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.
Domain	Globally defined domain name that the GSS queries when utilizing the NS keepalive.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.

Table 10-26 Field Descriptions for show statistics keepalive ns all Command (continued)

Field	Description
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Displaying TCP Keepalive Statistics

Use the **show statistics keepalive tcp** command to display statistics for configured TCP keepalive types managed by the GSS and used with VIP-type answers.

The syntax for the command is:

show statistics keepalive tcp {*ip_address* | **all** | **list**}

The options and variables are:

- *ip_address*—Specifies the IP address to display keepalive statistics.
- **all**—Displays all configured TCP-type keepalives.
- **list**—Lists all available IP addresses.

Table 10-27 describes the fields in the **show statistics keepalive tcp all** command output.

Table 10-27 Field Descriptions for show statistics keepalive tcp all Command

Field	Description
IP	IP address of the answer resource probed by the GSS.
Keepalive	IP address of the keepalive target.
Status	State of the keepalive. The possible states are Online, Offline, Init, and Suspended.

Table 10-27 Field Descriptions for show statistics keepalive tcp all Command (continued)

Field	Description
Keepalive Type	The Standard or Fast KAL-AP keepalive transmission rate used to define the failure detection time for the GSS.
Destination Port	Port on the remote device receiving the TCP keepalive request.
Packets Sent	Total number of keepalive packets sent to the answer by the GSS.
Packets Received	Total number of keepalive packets received by the GSS from the answer.
Positive Probe	Total number of keepalive probes sent to the answer that resulted in a positive (OK) response.
Negative Probe	Total number of keepalive probes sent to the answer that resulted in a negative response.
Transitions	Total number of keepalive transitions (for example, from Init to Online state) experienced by the keepalive.
GID	Global ID number used by the GSS.
LID	Local ID number used by the GSS.

Monitoring Network Proximity Statistics on a GSS

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 procedures:

- 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

Use the **show statistics dns proximity rule** command to display all proximity lookups by DNS rule name.

The syntax for the command is:

show statistics dns proximity rule

Table 10-28 describes the fields in the **show statistics dns proximity rule** command output.

Table 10-28 Field Descriptions for show statistics dns proximity rule Command

Field	Description
ProxRule	Name of the matched DNS rule
Proximity Hit Count	Number of DNS requests that match the DNS rule
Proximity Success Count	Number of DNS responses successfully returned with a proximate answer for the DNS rule

Displaying Proximity Database Statistics

Use the **show statistics proximity database** command to view the overall statistics on the proximity database, such as number of entries currently in the proximity database, the number of entries dropped, and the rate of lookups.

The syntax for the command is:

show statistics proximity database

Table 10-29 describes the fields in the **show statistics proximity database** command output.

Table 10-29 Field Descriptions for show statistics proximity database Command

Field	Description
Number of Entries in Use	Number of entries currently in the proximity database
Number of Add Entries Dropped	Number of entry creation requests that the GSS dropped because the proximity database limit had been reached
Max Number of Entries Used	Maximum number of entries used in the proximity database
Max Number of Entries Allowed	Maximum number of entries that the proximity database can hold (500,000 entries)
Number of Database Dump Started	Number of times the GSS initiated a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps
Number of Database Dump Completed	Number of times the GSS completed a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps
Number of Database Dump Failed	Number of times the GSS failed to perform a proximity database dump, including user-initiated database dumps and periodic system-initiated database dumps
Last Database Dump Started Time	The last time the GSS started a proximity database dump
Last Database Dump Failed Time	The last time the GSS failed to complete a proximity database dump
Number of Database Cleanup Started	Number of times the GSS initiated a database cleanup to remove the least recently used entries from the proximity database
Number of Database Cleanup Completed	Number of times the GSS completed a database cleanup to remove the least recently used entries from the proximity database

Table 10-29 Field Descriptions for show statistics proximity database Command (continued)

Field	Description
Number of Database Cleanup Failed	Number of times the GSS failed to cleanup the least recently used entries from the proximity database
Last Database Cleanup Started Time	The last time the GSS started the database cleanup process
Last Database Cleanup Failed Time	The last time the GSS failed to complete the database cleanup process

Displaying Proximity Group Statistics

Use the **show statistics proximity group-summary** command to display a summary of statistics for all configured proximity groups.

The syntax for the command is:

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 10-30 describes the fields in the **show statistics proximity group-summary** command output.

Table 10-30 Field Descriptions for show statistics proximity group-summary Command

Field	Description
Group Name	Unique alphanumeric name of the proximity group.
Target IP	Probe target IP address used by the proximity group, displayed in dotted-decimal notation.

Table 10-30 Field Descriptions for show statistics proximity group-summary Command (continued)

Field	Description
Total Entries	The total number of D-proxy IP address and subnet mask pairs contained in the proximity group.
Total Hits	Accumulated hit count for all entries in the proximity group. Increments when a match occurs for any proximity group entry in the group

Use the **show statistics proximity group-name** command to display statistics for a specific proximity group.

The syntax for the command is:

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 10-31 describes the fields in the **show statistics proximity group-name** command output.

Table 10-31 Field Descriptions for show statistics proximity group-name Command

Field	Description
Group Name	Unique alphanumeric name of the proximity group
Total Entries	The total number of D-proxy IP addresses or block of IP addresses included in the proximity group
Target IP	Probe target IP address used by the proximity group, displayed in dotted-decimal notation.
Address	D-proxy IP address included in the proximity group
Prefix	Subnet mask used to specify the block of IP addresses included in the proximity group, displayed as an integer (for example, 24 or 32)

Table 10-31 Field Descriptions for show statistics proximity group-name Command (continued)

Field	Description
Hit Counts	Increments when a match occurs for this proximity group entry
Last Hit Time	The last time the hit count incremented due to an entry match

Displaying Proximity Lookup Statistics

Use the **show statistics proximity lookup** command to display statistics about the proximity lookups that have occurred on this GSS.

The syntax for the command is:

show statistics proximity lookup

Table 10-32 describes the fields in the **show statistics proximity lookup** command output.

Table 10-32 Field Descriptions for show statistics proximity lookup Command

Field	Description
Total lookup requests	Total number of proximity lookup requests made to the proximity database
Database entry not found	Number of times the GSS was unable to locate a proximate answer in the database
Partial RTT data returned	Number of times only partial round-trip time (RTT) data was returned to the DNS service by the proximity subsystem
Current lookup request rate	Current request rate per second that requests are made by the DNS service to perform a proximity lookup in the database
Peak lookup request rate	Peak request rate per second that requests are made by the DNS service to perform a proximity lookup in the database

Table 10-32 Field Descriptions for show statistics proximity lookup Command (continued)

Field	Description
Lookup failed due to database full	Number of times the GSS was unable to complete a proximity lookup because the database exceeded the maximum number of entries
Last database full happened	Last time the proximity database was full

Displaying Proximity Probe Transfer Statistics

Use the **show statistics proximity probes** command to display general probe success and failure counts.

The syntax for the command is:

show statistics proximity probes

Table 10-33 describes the fields in the **show statistics proximity probes** command output.

Table 10-33 Field Descriptions for show statistics proximity probes Command

Field	Description
Authentication	Indicates whether the GSS performs DRP authentication when exchanging packets with the DRP agent in a probing device. States are Enabled and Disabled.
Echo Rx	Number of DRP echo responses received by the GSS from all configured probing devices.
Echo Tx	Number of DRP echo requests sent by the GSS to all configured probing devices.
Measure Rx	Number of DRP measured requests received by the GSS from all configured probing devices.
Measure Tx	Number of DRP measured requests sent by the GSS to all configured probing devices.

Table 10-33 Field Descriptions for show statistics proximity probes Command

Field	Description
Pkts Rx	Total number of DRP packets received by the GSS from all configured probing devices.
Pkts Tx	Number of DRP packets sent by the GSS to all configured probing devices.

Use the **show statistics proximity probes detailed** command to display detailed statistics for the ICMP and TCP probes relative to all configured zones. This command also displays the operating status of the primary and secondary probing devices (ONLINE or OFFLINE).

The syntax for the command is:

show statistics proximity probes detailed

Table 10-34 describes the fields in the **show statistics proximity probes detailed** command output.

Table 10-34 Field Descriptions for show statistics proximity probes detailed Command

Field	Description
Zone ID	Numerical identifier of the proximity zone
Zone Name	Name of the proximity zone
Authentication	Indicates if the GSS performs DRP authentication when exchanging packets with the DRP agent in a probing device
Primary	Identifies the IP address of the primary probing device servicing this zone and the status of the probing device (ONLINE or OFFLINE)
Secondary	Identifies the IP address of the backup probing device servicing this zone and the status of the probing device (ONLINE or OFFLINE)
Echo Rx	Number of DRP echo responses received by the GSS from all configured probing devices

Table 10-34 Field Descriptions for show statistics proximity probes detailed Command (continued)

Field	Description
Echo Tx	Number of DRP echo requests sent by the GSS to all configured probing devices
Measure Rx	Number of DRP measured requests received by the GSS from all configured probing devices
Measure Tx	Number of DRP measured requests sent by the GSS to all configured probing devices
Pkts Rx	Total number of DRP packets received by the GSS from the probing device in the proximity zone
Pkts Tx	Number of DRP packets sent by the GSS to the probing device in the proximity zone
Pkts Rx Rate	Current received request rate per second
Pkts Tx Rate	Current transmitted request rate per second
Peak Rx Rate	Peak received request rate per second
Peak Tx Rate	Peak transmitted request rate per second

Displaying Proximity Status

Use the **show proximity** command to display general status information about the proximity subsystem.

The syntax for the command is:

show proximity

Table 10-35 describes the fields in the **show proximity** command output.

Table 10-35 Field Descriptions for show proximity Command

Field	Description
Proximity subsystem status	Current operating status of the Proximity subsystem component
Proximity database dump interval	Time period between automatic proximity database dumps performed by the GSS
Proximity database age-out interval	Time period between checks by the GSS to verify when the user-configured entry inactivity timeout value elapses

Displaying Proximity Group Configuration

Use the **show proximity group-summary** command to display a summary of all configured proximity groups.

Note This command displays the configuration output to the console only if the number of proximity elements, or IP blocks, is less than 1000. (This value is not configurable). If the number of proximity elements is more than 1000, an error message displays asking you to execute the **proximity group-summary dump** *filename* command.

Table 10-36 describes the fields in the **show proximity group-summary** command output.

Table 10-36 Field Descriptions for show proximity group-summary Command

Field	Description
Name	Unique alphanumeric name of the proximity group
Address Blocks	IP address block of the proximity group, specified in dotted-decimal notation

Use the **show proximity group-name** command to display the configuration of a specific proximity group.

The syntax for the command is:

show proximity group-name {*groupname*}

Enter the exact name of a proximity group to display all proximity entries related to that group.

Table 10-37 describes the fields in the **show proximity group-name** command output.

Table 10-37 Field Descriptions for show proximity group-name Command

Field	Description
Name	Unique alphanumeric name of the proximity group
Address Blocks	IP address block of the proximity group, specified in dotted-decimal notation

Displaying Proximity Database Status

Use the **show proximity database** command to display proximity the database entries by specifying one or more entry matching criteria.

The syntax for this command is:

show proximity database {**all** | **assigned** | **group** {*name*} | **inactive** *minutes* | **ip** {*ip-address*} **netmask** {*netmask*} | **no-rtt** | **probed**}

The options and variables are:

- **all**—Displays all entries in the proximity database.
- **assigned**—Displays all static entries in the proximity database.
- **group** *name*—Displays all entries that belong to a named proximity group. Specify the exact name of a previously created proximity group.
- **inactive** *minutes*—Displays all dynamic entries that have been inactive for a specified time. Valid values are 0 to 43200 minutes.
- **ip** *ip-address* **netmask** *netmask*—Displays all proximity entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **no-rtt**—Displays all entries in the PDB that do not have valid RTT values.
- **probed**—Displays all dynamic entries in the PDB.

For example, to display entries related to the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gss1.example.com# show proximity database ip 192.168.8.0 255.255.255.0
```

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 procedures:

- Displaying DNS Rule Sticky Statistics
- Displaying Sticky Statistics
- Displaying Global Sticky Statistics
- Displaying Global Sticky Mesh Statistics
- Displaying Sticky Group Statistics
- Displaying Sticky Status
- Displaying Sticky Database Status
- Displaying Global Sticky Operating Status
- Displaying Global Sticky Mesh Operating Status
- Displaying Sticky Group Configuration

Displaying DNS Rule Sticky Statistics

Use the **show statistics dns sticky rule** command to display all DNS sticky lookups by DNS rule name.

The syntax for the command is:

show statistics dns sticky rule

Table 10-38 describes the fields in the **show statistics dns sticky rule** command output.

Table 10-38 Field Descriptions for show statistics dns sticky rule Command

Field	Description
Rule	Name of the matched DNS rule
Hits	Total number of successful lookups in the sticky database for the sticky database entry
Misses	Total number of failed lookups in the sticky database for the DNS rule
Additions	Total number of times that a request matched on a DNS rule, resulting in the GSS adding an entry to the sticky database

Displaying Sticky Statistics

Use the **show statistics sticky** command to 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.

The syntax for the command is:

show statistics sticky

Table 10-39 describes the fields in the **show statistics sticky** command output.

Table 10-39 Field Descriptions for show statistics sticky Command

Field	Description
Current entry count	Current number of entries in the sticky database.
Highest entry count	Maximum number of entries in the sticky database since the last time sticky was enabled or the sticky statistics were cleared.
Total Lookups	Total number of lookups in the sticky database.
Hits	Number of successful lookups in the sticky database.
Misses	Number of failed lookups in the sticky database.

Table 10-39 Field Descriptions for show statistics sticky Command (continued)

Field	Description
Addition success	Number of addition requests for the sticky database that succeeded.
Addition fail	Number of addition requests for the sticky database that failed. The sticky database will not accept further addition requests when the database is full, you stop DNS sticky through the **sticky stop** CLI command, or there has been an internal error.
Modification success	Number of answer modification requests that succeeded.
Modification fail	Number of answer modification requests that failed.
Timeouts	Number of entries removed from the sticky database because the answer exceeded the user-configured Entry Inactivity Timeout value.
Reclaimed	Number of entries removed from the sticky database due to overflow.
CLI deletions local	Number of entries manually deleted from the sticky database through the **sticky database delete** CLI command, entered on the local GSS node.
CLI deletions remote	Number of entries manually deleted from the sticky database through the **sticky database delete** CLI command, entered on a GSS peer.

Displaying Global Sticky Statistics

Use the **show statistics sticky global** command to display a summary of counter statistics for global sticky messaging between the local GSS node and its GSS peers.

The syntax for the command is:

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 10-40 describes the fields in the **show statistics sticky global** command output.

Table 10-40 Field Descriptions for show statistics sticky global Command

Field	Description
Entry Type	Statistics on sticky database entry operations performed by the local GSS node.
Send OK	Sticky database entry messages transmitted by the local GSS node without a failure.
Send Fail	Sticky database entry messages transmitted by the local GSS node with errors.
Received	Sticky database entry messages received by the local GSS node from GSS peers.
Add	Number of new entries added to the sticky database of the local GSS node.
Modify	Number of sticky database entries modified by the local GSS node due to a keepalive failure.
Lookup Fast	Number of sticky database entries in the local GSS node that had their sticky inactivity time reset to an initial value because the GSS performed a fast lookup. A GSS performs a fast lookup when adding new entries to the sticky database, deleting entries from the sticky database, or when the sticky expiration time is less than five minutes.
Lookup Slow	Number of sticky database entries in the local GSS node that had their sticky inactivity time reset to an initial value because the GSS performed a slow lookup. A GSS performs a slow lookup when the sticky expiration time is greater than five minutes.

Table 10-40 Field Descriptions for show statistics sticky global Command (continued)

Field	Description
Remove	Number of entries removed from the sticky database of the local GSS node through the **sticky database delete** command. Entries removed by the **sticky database delete all** command are reflected in the Remove All field (see below).
Add Sync	Number of entries added to the sticky database of the local GSS node due to the result of a peer synchronization, not due to a normal DNS client request.
Message Type	Statistics on sticky database messages sent or received by the local GSS node.
Send OK	Messages transmitted by the local GSS node without a failure.
Send Fail	Messages transmitted by the local GSS node with errors.
Received	Messages received by the local GSS node from GSS peers.
Add	Number of Add entry type messages sent or received by the local GSS node.
Modify	Number of Modify entry type messages sent or received by the local GSS node.
Lookup Fast	Number of Lookup Fast entry type messages sent or received by the local GSS node.
Lookup Slow	Number of Lookup Slow entry type messages sent or received by the local GSS node.
Remove	Number of Remove messages sent or received by the the local GSS node.
Add Sync	Number of Add Sync entry type messages sent or received by the local GSS node.

Table 10-40 Field Descriptions for show statistics sticky global Command (continued)

Field	Description
Remove All	Number of times the **sticky database delete all** command has been entered on the local GSS node to delete all entries from the sticky database. The Remove All count includes the number of Remove All messages sent and received by the local GSS node.
Request Db	Number of times the local GSS node sent a Request Db message to a GSS peer, or received a Request Db message from a GSS peer, requesting to share the contents of its sticky database upon startup.
Ack RequestDb	Number of times the local GSS node sent an Ack RequestDb message to a GSS peer, or received an Ack RequestDb message from a GSS peer, to acknowledge that it received a request to share the contents of its sticky database upon startup.
Refuse Db Req	Number of times the local GSS node sent a Refuse Db Req message to a GSS peer, or received a Refuse Db Req message from a GSS peer, indicating a refusal to share the contents of its sticky database upon startup. A GSS, typically, refuses to share the contents of its local database while in the process of performing a database synchronization.
Sync Start	Number of times the Sync Start message has been sent or received by the local GSS node. The GSS uses the Sync Start message to lock out certain critical functions (such as the use of the **sticky database delete** command) while any GSS within the mesh is performing a synchronization. When the Sync Start message arrives, the GSS blocks all sticky database entry deletions until it either receives the Sync Done message or an internal timer expires.

Table 10-40 Field Descriptions for show statistics sticky global Command (continued)

Field	Description
Sync Done	Number of times the Sync Done message has been sent or received by the local GSS node. The GSS uses the Sync Done message to lock out certain critical functions (such as the use of the **sticky database delete** command) while any GSS within the mesh is performing a synchronization.
Version mis-match	Error message indicating the number of times the local GSS node was unable to communicate with a peer due to different versions of GSS software.
Clock Out Of Sync	Error message indicating the number of times the local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by greater than three minutes with the other GSS peers ignores update messages from all peers until you re-synchronize its system clock (see Chapter 8, Configuring DNS Sticky, for details).
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 8, Configuring DNS Sticky, for details).

Displaying Global Sticky Mesh Statistics

Use the **show statistics sticky mesh** CLI command to display detailed statistics for each GSS peer in the global sticky mesh.

Table 10-41 describes the fields in the **show statistics sticky mesh** command output.

Table 10-41 Field Descriptions for show statistics sticky mesh Command

Field	Description
Mesh Information for application sticky	Status and statistics about the global sticky mesh
Transmit Pkts	Total number of application data packets transmitted by the local GSS node to GSS peers in the mesh
Transmit Bytes	Total number of application data bytes transmitted by the local GSS node to GSS peers in the mesh
Receive Pkts	Total number of application data packets received by the local GSS node from GSS peers in the mesh
Receive Bytes	Total number of application data bytes received by the local GSS node from GSS peers in the mesh
Dropped Tx Pkts	Total number of packets to be transmitted by the local GSS node but were dropped due to buffer errors
Dropped Rx Pkts	Total number of packets received by the local GSS node but were dropped due to buffer errors
Current TxQueue	Total number of packets in the buffer transmit queue of the local GSS node that are waiting to be transmitted
Maximum TxQueue	Maximum number of packets that have been in the buffer transmit queue of the local GSS node
Current RxQueue	Total number of packets in the buffer receive queue of the local GSS node that are waiting to be received
Maximum RxQueue	Maximum number of packets that have been in the buffer receive queue of the local GSS node

Table 10-41 Field Descriptions for show statistics sticky mesh Command (continued)

Field	Description
Buffers Alloc'd	Number of optimal-sized frames allocated for the buffer transmit and buffer receive data
Buffers Free	Number of buffers currently free in the local GSS node
Session Information for *GSS peer*	Status and statistics for a specific GSS peer in the mesh
GSS ID	Unique identifier of the GSS peer in the mesh.
CurTx Data Pkts	Number of data packets sent by the local GSS node to the GSS peer during the current session
CurTx Data Bytes	Number of data bytes sent by the local GSS node to the GSS peer during the current session
TtlTx Data Pkts	Number of application data packets sent by the local GSS node to the GSS peer for the total duration of the mesh
TtlTx Data Bytes	Number of application data bytes sent by the local GSS node to the GSS peer for the total duration of the mesh
Transmit Pkts	Total number of packets transmitted from the local GSS node to the GSS peer (including application packets, control packets, RTT packets, and keepalive packets)
Transmit Bytes	Total number of bytes transmitted from the local GSS node to the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes)
CurRx Data Pkts	Number of data packets received by the local GSS node from the GSS peer during the current session
CurRx Data Bytes	Number of data bytes received by the local GSS node from the GSS peer during the current session
TtlRx Data Pkts	Number of application data packets received by the local GSS node from the GSS peer for the total duration of the mesh

Table 10-41 Field Descriptions for show statistics sticky mesh Command (continued)

Field	Description
TtlRx Data Bytes	Number of application data bytes received by the local GSS node from the GSS peer for the total duration of the mesh
Receive Pkts	Total number of packets received by the local GSS node from the GSS peer (including application packets, control packets, RTT packets, and keepalive packets)
Receive Bytes	Total number of bytes received by the local GSS node from the GSS peer (including application bytes, control bytes, RTT bytes, and keepalive bytes)
ConnectFailures	Number of times that the connection attempt failed between the local GSS node and the GSS peer
CurConnAttempts	Number of current connection attempts between the local GSS node and the GSS peer
ConnectRejects	Number of connections rejected by the GSS peer
ConnectDeclines	Number of connections declined by the local GSS node.

Displaying Sticky Group Statistics

Use the **show statistics sticky group-summary** command to display a summary of statistics for all configured sticky groups.

Table 10-42 describes the fields in the **show statistics sticky group-summary** command output.

Table 10-42 Field Descriptions for show statistics sticky group-summary Command

Field	Description
Group Name	Unique alphanumeric name of the DNS sticky group.
Group Number	IP address block of the sticky group, specified in dotted-decimal notation.

Table 10-42 Field Descriptions for show statistics sticky group-summary Command (continued)

Field	Description
Total Entries	The total number of D-proxy IP address and subnet mask pairs contained in the sticky group.
Total Hits	Accumulated hit count for all entries in the sticky group. Increments when a match occurs for each sticky group entry

Use the **show statistics sticky group-name** command to display statistics for a specific sticky group.

The syntax for the command is:

show statistics sticky group-name {*groupname*}

Enter the exact name of a sticky group to display all sticky entries related to that group.

Table 10-43 describes the fields in the **show statistics sticky group-name** command output.

Table 10-43 Field Descriptions for show statistics sticky group-name Command

Field	Description
Group Name	Unique alphanumeric name of the DNS sticky group
Group Number	IP address block of the sticky group, specified in dotted-decimal notation
Total Entries for Group	The total number of D-proxy IP addresses included in the sticky group
Address	D-proxy IP address included in the sticky group
Prefix	Subnet mask included in the sticky group, displayed as an integer (for example, 24 or 32)
Hit Count	Increments when a match occurs for this sticky group entry
Last Time Hit	The last time the hit count incremented due to an entry match

Displaying Sticky Status

Use the **show sticky** command to display general status information about the sticky subsystem.

The syntax for the command is:

show sticky

Table 10-44 describes the fields in the **show sticky** command output.

Table 10-44 Field Descriptions for show sticky Command

Field	Description
Sticky Manager status	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 include: • **Initializing**—Appears only during boot time or after entering the **gss start** CLI command. • **Disabled via GUI**—Appears after you disable sticky from the primary GSSM GUI. • **Stopped via CLI**—Appears after you enter the **sticky stop** CLI command. • **Ready in Local mode**—Appears when the GSS is configured for sticky Local mode from the primary GSSM GUI and the GSS software is running. • **Ready in Global mode**—Appears when the GSS is configured for sticky Global mode from the primary GSSM GUI and the GSS software is running.
Database entry count	Current number of entries in the sticky database.

Table 10-44 Field Descriptions for show sticky Command (continued)

Field	Description
Dump status	Current sticky database dump subsystem status of the GSS. The GSS automatically dumps sticky database entries to a backup file on disk approximately every 20 minutes. The Dump status messages include: Initialized, Disabled, Waiting, and In Progress.
Dump interval	Time period between automatic sticky database dumps performed by the GSS.
Reclaim status	Current operating status of the overflow recovery subsystem. The Reclaim status messages include: Initialized, Disabled, Waiting, and In Progress.
Timeout status	Current operating status of the entry inactivity timeout subsystem. The Timeout status messages include: Initialized, Disabled, Waiting, and In Progress.
Timeout interval	Time period between checks by the GSS to verify when the user-configured sticky inactivity timeout value elapses.
Mesh status	Current operating status of the sticky global mesh. Status messages include: • **Running**—The GSS is operating properly in the sticky mesh. • **Failed**—The GSS is unable to operate properly in the sticky mesh. • **Waiting**—The GSS is waiting for mesh configuration information. • **Enabled**—Global sticky is enabled on the local GSS node. • **Disabled**—Global sticky is disabled on the local GSS node (either from the primary GSSM GUI or through the **sticky stop** CLI command).

Displaying Sticky Database Status

Use the **show sticky database** command to display sticky database entries by specifying one or more entry matching criteria.

The syntax for the command is:

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 options and variables are:

- **all**—Displays all sticky entries in the sticky database.
- **answer** *name/ip_address*—Displays all sticky entries related to a particular answer. Specify the name of the answer. If there is no name for the answer, specify the IP address of the sticky answer in dotted-decimal notation (for example, 192.168.9.0).
- **domain** *name*—Displays all sticky entries related to a domain. Specify the exact name of a previously created domain.
- **domain-list** *name*—Displays all sticky entries related to a domain list. Specify the exact name of a previously created domain list.
- **group** *name*—Displays all sticky entries related to a sticky group. Specify the exact name of a previously created sticky group.
- **inactive minimum** *minutes* **maximum** *minutes*—Displays all sticky entries that have not received a client hit in the time interval between the specified minimum and maximum values, entered in minutes. Enter a value from 0 to 10100 minutes (seven days) as the specified minimum value and maximum value.
- **ip** *ip_address* **netmask** *netmask*—Displays all sticky entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **rule** *rulename*—Displays all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

Table 10-45 describes the fields in the **show sticky database all** command output.

Table 10-45 Field Descriptions for show sticky database Command

Field	Description
Client/Group	IP address of client D-proxy or name of sticky group
Domain/DL	Name of the hosted domain (including wildcards) or the name of a matched domain list (DL)
Rule	Name of the DNS rule that was matched to add this entry
Answer	VIP address of the answer (VIP-type answer)
SIT	User-specified sticky interval timeout (SIT) value
TTL	The remaining time that the entry in the sticky database is valid
Hits	Total number of successful lookups in the sticky database for the sticky database entry

Displaying Global Sticky Operating Status

Use the **show sticky global** command to display the most recent sticky database message identifiers sent by the local GSS node and received from its GSS mesh peers. 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** option.

The syntax for the command is:

show sticky global {**verbose**}

Table 10-46 describes the fields in the **show sticky global** command output.

Table 10-46 Field Descriptions for show sticky global Command

Field	Description
Mesh Peer Count	Total number of GSS peers in a sticky mesh (not including the local GSS node).
Last Message ID Sent for Each Mesage Type	Summary of the unique global sticky message identifiers last sent by the local GSS node.
Add	Unique identifier of the last Add entry-type message sent by the local GSS node.
Modify	Unique identifier of the last Modify entry-type message sent by the local GSS node.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.
Details of Most Recently Received Messages by Peer	Status summary of the global sticky message identifiers last received by the local GSS node.
Peer Name	Host name of the GSS peer in the mesh.
Peer ID	Unique identifier of the GSS peer in the mesh.
Last Type	Type of the message last received from the peer.

Table 10-46 Field Descriptions for show sticky global Command (continued)

Field	Description
Last Status	Status of the last message received from the peer. Status messages include: • **Received OK**—Message was received and processed • **Version mismatch**—Message dropped because the local GSS node was unable to communicate with a peer due to different versions of GSS software. • **Clock out of sync**—The local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by greater than three minutes with the other GSS peers ignores update messages from all peers until you re-synchronize its system clock (see Chapter 8, Configuring DNS Sticky, for details). • **Mask mismatch**—The local GSS node was unable to communicate with a peer due to a difference in global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure. Refer to Chapter 8, Configuring DNS Sticky, for details about globally configuring the subnet mask of all GSS devices in the mesh from the primary GSSM GUI.
Last MessageID Received for each Message Type...	Summary of the unique global sticky messages last received by the local GSS node from each GSS mesh peer.
Add	Unique identifier of the last Add entry-type message received by the local GSS node from the GSS peer.

Table 10-46 Field Descriptions for show sticky global Command (continued)

Field	Description
Modify	Unique identifier of the last Modify entry-type message received by the local GSS node from the GSS peer.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message received by the local GSS node from the GSS peer.

Table 10-47 describes the fields in the **show sticky global verbose** command output.

Table 10-47 Field Descriptions for show sticky global verbose Command

Field	Description
Mesh Peer Count	Total number of GSS peers in a sticky mesh (not including the local GSS node).
Last Message ID Sent for Each Mesage Type	Summary of the unique global sticky message identifiers last sent by the local GSS node.
Add	Unique identifier of the last Add entry-type message sent by the local GSS node.
Modify	Unique identifier of the last Modify entry-type message sent by the local GSS node.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message sent by the local GSS node.
Lookup Slow	Unique identifier of the last Lookup Slow entry-type message sent by the local GSS node.
Remove	Unique identifier of the last Remove entry-type message sent by the local GSS node.
Add Sync	Unique identifier of the last Add Sync entry-type message sent by the local GSS node.
Remove All	Unique identifier of the last Remove All message sent by the local GSS node.

Table 10-47 Field Descriptions for show sticky global verbose Command (continued)

Field	Description
Request Db	Unique identifier of the last Request Db message sent by the local GSS node.
Ack ReqDb	Unique identifier of the last Ack ReqDb message sent by the local GSS node.
Refuse ReqDb	Unique identifier of the last Refuse ReqDb message sent by the local GSS node.
Sync Start	Unique identifier of the last Sync Start message sent by the local GSS node.
Sync Done	Unique identifier of the last Sync Done message sent by the local GSS node.
Details of Most Recently Received Messages by Peer	Status summary of the global sticky message identifiers last received by the local GSS node.
Peer Name	Host name of the GSS peer in the mesh.
Peer ID	Unique identifier of the GSS peer in the mesh.
Last Type	Type of the message last received from the peer

Table 10-47 Field Descriptions for show sticky global verbose Command (continued)

Field	Description
Last Status	Status of the last message received from the peer. Status messages include: • **Received OK**—Message was received and processed • **Version mismatch**—Message dropped because the local GSS node was unable to communicate with a peer due to different versions of GSS software. • **Clock out of sync**—The local GSS node was unable to communicate with a peer due to clock synchronization issues. A GSS that has a system clock that is out of synchronization by greater than three minutes with the other GSS peers ignores update messages from all peers until you re-synchronize its system clock (see Chapter 8, Configuring DNS Sticky, for details). • **Mask mismatch**—The local GSS node was unable to communicate with a peer due to a difference in global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure. Refer to Chapter 8, Configuring DNS Sticky, for details about globally configuring the subnet mask of all GSS devices in the mesh from the primary GSSM GUI .
Last MessageID Received for each Message Type...	Summary of the unique global sticky messages last received by the local GSS node from each GSS mesh peer.

Table 10-47 Field Descriptions for show sticky global verbose Command (continued)

Field	Description
Add	Unique identifier of the last Add entry-type message received by the local GSS node from the GSS peer.
Modify	Unique identifier of the last Modify entry-type message received by the local GSS node from the GSS peer.
Lookup Fast	Unique identifier of the last Lookup Fast entry-type message received by the local GSS node from the GSS peer.
Lookup Slow	Unique identifier of the last Lookup Slow entry-type message received by the local GSS node from the GSS peer.
Remove	Unique identifier of the last Remove entry-type message received by the local GSS node from the GSS peer.
Add Sync	Unique identifier of the last Add Sync entry-type message received by the local GSS node from the GSS peer.
Remove All	Unique identifier of the last Remove All message received by the local GSS node from the GSS peer.
Request Db	Unique identifier of the last Request Db message received by the local GSS node from the GSS peer.
Ack ReqDb	Unique identifier of the last Ack RegDb message received by the local GSS node from the GSS peer.
Refuse Db	Unique identifier of the last Refuse ReqDb message received by the local GSS node from the GSS peer.
Sync Start	Unique identifier of the last Sync Start message received by the local GSS node from the GSS peer.
Sync Done	Unique identifier of the last Sync Done message received by the local GSS node from the GSS peer.

Displaying Global Sticky Mesh Operating Status

To display sticky mesh status information locally from the CLI of a GSS, use 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:

- **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 10-48 describes the fields in the **show sticky mesh** command output.

Table 10-48 Field Descriptions for show sticky mesh Command

Field	Description
My GSS ID	Unique identifier of the local GSS node in the mesh.
Mesh ID	Unique identifier of the global sticky mesh.
Port	TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user-configurable.
Remote GSS IP Address/Host Name	IP address or host name of the GSS peer in the mesh.

Table 10-48 Field Descriptions for show sticky mesh Command (continued)

Field	Description
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.
State	State of the communication link between the local GSS node and the mesh peer. The possible states include: • **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 10-49 describes the fields in the **show sticky mesh session** command output.

Table 10-49 Field Descriptions for show sticky mesh session Command

Field	Description
Session Information for *GSS peer*	Identifies the host name of the GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.
RTT	Application-level round-trip time (RTT) between the local GSS node and the mesh peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.

Table 10-49 Field Descriptions for show sticky mesh session Command (continued)

Field	Description
State	State of the communication link between the local GSS node and the mesh peer. The possible states include: • **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 10-50 describes the fields in the **show sticky mesh session verbose** command output.

Table 10-50 Field Descriptions for show sticky mesh session verbose Command

Field	Description
Session Information for *GSS peer*	Identifies the host name of the GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.

Table 10-50 Field Descriptions for show sticky mesh session verbose Command (continued)

Field	Description
Session State	State of the communication link between the local GSS node and the mesh peer. The possible states include: • **SESSION_STOP**—Indicates that the session is dead • **SESSION_INIT**—Indicates that the session is initializing • **SESSION_OPEN**—Indicates that the connection to the peer has been made • **SESSION_AUTH**—Indicates that authentication is occurring • **SESSION_UP**—Indicates that the session is up • **SESSION_DOWN**—Indicates that the session is down or failing
RTT	Application-level round-trip time (RTT) between the local GSS node and the mesh peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.
Encrypt Type	Encryption method performed on the data packets. The method is either: • **md5hash**—MD5-based hashing encryption method • **none**—No encryption Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, Configuring DNS Sticky for details.

Table 10-50 Field Descriptions for show sticky mesh session verbose Command (continued)

Field	Description
Authentication	Authentication method performed by the GSS peer to prevent unauthorized access. The method is either: • **challenge**—Challenge Handshake Authentication Protocol (CHAP) • **none**—No secret string used for authentication Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, Configuring DNS Sticky for details.
KalFreq	Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user-configurable.
Max FrameSize	The maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user-configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user-configurable.
PrePend	Allocated header size in the buffer. The header size is always eight bytes.
IP Address	IP address of the GSS peer in the mesh.
GSS ID	Unique identifier of the GSS peer in the mesh.
Connect from IP	Actual IP network address of the GSS peer in the mesh.
My Local Address Via Peer	IP address of the local GSS node as seen by the GSS peer.
Last Up Event	The day and time of the most recent Up event.
Last Down Event	The day and time of the most recent Down event.
FSM Events	Finite State Machine events as related to the Session State field.
STOP	Number of SESSION_STOP events.

Table 10-50 Field Descriptions for show sticky mesh session verbose Command (continued)

Field	Description
INIT	Number of SESSION_INIT events.
OPEN	Number of SESSION_OPEN events.
AUTH	Number of SESSION_AUTH events.
UP	Number of SESSION_UP events.
DOWN	Number of SESSION_DOWN events.

Table 10-51 describes the fields in the **show sticky mesh verbose** command output.

Table 10-51 Field Descriptions for show sticky mesh verbose Command

Field	Description
Mesh Information for application sticky	Status and statistics about the global sticky mesh.
My GSS ID	Unique identifier of the local GSS node in the mesh.
Mesh ID	Unique identifier of the global sticky mesh.
Port	TCP port used by all GSS devices connected in the sticky mesh. This parameter is not user-configurable.
Encrypt Type	Encryption method performed on the data packets. The method is either: • **md5hash**—MD5-based hashing encryption method • **none**—No encryption Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, Configuring DNS Sticky for details.

Table 10-51 Field Descriptions for show sticky mesh verbose Command (continued)

Field	Description
Authentication	Authentication method performed by GSS peers to prevent unauthorized access. The method is either: • **challenge**—Challenge Handshake Authentication Protocol (CHAP) • **none**—No secret string used for authentication Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, 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 "default".
MaxFrameSize	The maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user-configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user-configurable.
Max Rate	Maximum rate that the local GSS node can transmit packets to GSS peers in the mesh.
Favored Peer	Identifies the favored GSS peer for the local GSS node, specified on the Global Sticky Configuration details page of the primary GSSM GUI. A favored peer enables you to force a faster synchronization of sticky database entries with a specific GSS peer upon reentry into the sticky mesh. If you did not specify a favored peer, the GSS displays "No Favored Peer configured".
Session Information for *GSS peer*	Status and statistics for a specific GSS peer in the mesh.
Session ID	Unique identifier of the point-to-point connection between the local GSS node and the mesh peer.

Table 10-51 Field Descriptions for show sticky mesh verbose Command (continued)

Field	Description
Session State	State of the communication link between the local GSS node and the mesh peer. The possible states include: • **SESSION_STOP**—Indicates that the session is dead • **SESSION_INIT**—Indicates that the session is initializing • **SESSION_OPEN**—Indicates that the connection to the peer has been made • **SESSION_AUTH**—Indicates that authentication is occurring • **SESSION_UP**—Indicates that the session is up • **SESSION_DOWN**—Indicates that the session is down or failing
RTT	Application-level round-trip time (RTT) between the local GSS node and this GSS peer. If the GSS has not yet made an RTT measurement, the GSS displays "--" in the field.
Encrypt Type	Encryption method performed on the data packets. The method is either: • **md5hash**—MD5-based hashing encryption method • **none**—No encryption Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, Configuring DNS Sticky for details.

Table 10-51 Field Descriptions for show sticky mesh verbose Command (continued)

Field	Description
Authentication	Authentication method performed by GSS peers to prevent unauthorized access. The method is either: • **challenge**—Challenge Handshake Authentication Protocol (CHAP) • **none**—No secret string used for authentication Refer to the "Configuring the Global Sticky Mesh" section in Chapter 8, Configuring DNS Sticky for details.
KalFreq	Time in seconds between sending keepalive messages from the local GSS node to this GSS peer. This parameter is not user-configurable.
Max FrameSize	The maximum frame size allowed for communication between GSS devices in the mesh. This parameter is not user-configurable.
OptmlFrameSize	Optimal frame size for communication between GSS devices in the mesh. This parameter is not user-configurable.
PrePend	Allocated header size in the buffer. The header size is always eight bytes.
IP Address	IP address of the GSS peer in the mesh.
GSS ID	Unique identifier of the GSS peer in the mesh.
Connect from IP	Actual IP network address of the GSS peer in the mesh.
My Local Address Via Peer	IP address of the local GSS node as seen by the GSS peer.
Last Up Event	The day and time of the most recent Up event.
Last Down Event	The day and time of the most recent Down event.
FSM Events	Finite State Machine events as related to the Session State field.
STOP	Number of SESSION_STOP events.

Table 10-51 Field Descriptions for show sticky mesh verbose Command (continued)

Field	Description
INIT	Number of SESSION_INIT events.
OPEN	Number of SESSION_OPEN events.
AUTH	Number of SESSION_AUTH events.
UP	Number of SESSION_UP events.
DOWN	Number of SESSION_DOWN events.

Displaying Sticky Group Configuration

Use the **show sticky group-summary** command to display a summary of all configured sticky groups.

Table 10-52 describes the fields in the **show sticky group-summary** command output.

Table 10-52 Field Descriptions for show sticky group-summary Command

Field	Description
Name	Unique alphanumeric name of the DNS sticky group
Address Blocks	IP address block of the sticky group, specified in dotted-decimal notation

Use the **show sticky group-name** command to display the configuration of a specific sticky group.

The syntax for the command is:

show sticky group-name {*groupname*}

Enter the exact name of a sticky group to display all sticky entries related to that group.

Table 10-53 describes the fields in the **show sticky group-name** command output.

Table 10-53 Field Descriptions for show sticky group-name Command

Field	Description
Name	Unique alphanumeric name of the DNS sticky group
Address Blocks	IP address block of the sticky group, specified in dotted-decimal notation

Clearing GSS Global Server Load-Balancing Statistics

Use the **clear statistics** command to reset global server load-balancing statistics for one or more of your GSS components. Clearing the statistics for a GSS component erases all record of routing activity and performance for that device.

The syntax for the **clear statistics** command is:

clear statistics {**boomerang** | **ddos** [**all** | **attacks** | **drops** | **global**] | **dns** | **drpagent** | **keepalive** {**all** | **cra** | **http-head** | **icmp** | **kalap** | **ns** | **scripted-kal** | **tcp**} | **proximity** | **sticky** {**mesh**}}

The options are:

- **statistics**—Resets load-balancing statistics about the GSS
- **boomerang**—Resets statistics relating to the Boomerang server component of the GSS
- **ddos**—Resets statistics relating 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 relating to the DNS server component of the GSS, including proximity and sticky DNS rule statistics.
- **drpagent**—Resets statistics relating to the DRP agent component of the GSS.
- **keepalive**—Resets statistics relating to the keepalive function of the GSS software
- **all**—Resets statistics for all keepalive types maintained by the GSS

- **cra**—Resets statistics for only CRA-type keepalives maintained by the GSS
- **http-head**—Resets statistics for only the VIP HTTP-HEAD type keepalive maintained by the GSS
- **icmp**—Resets statistics for only the VIP ICMP-type keepalive maintained by the GSS
- **kalap**—Resets statistics for only the VIP KAL-AP-type keepalive maintained by the GSS
- **ns**—Resets statistics for the Name Server-type keepalive maintained by the GSS
- **scripted-kal**—Resets statistics for the Scripted-Kal -type keepalive maintained by the GSS.
- **tcp**—Resets statistics for the IP and port TCP-type keepalive maintained by the GSS
- **proximity**—Resets statistics for the network proximity function
- **sticky**—Resets statistics for the DNS sticky function
- **mesh**—Resets sticky global mesh and session statistics for the local GSS node of the mesh

For example:

```
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 includes the following procedures:

- Monitor 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

Monitor Answer Status and Statistics

The Answers section of the Monitoring tab displays statistics for 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 procedures:

- Monitoring Answer Hit Counts
- Monitoring Answer Keepalive Statistics
- Monitoring Answer Status

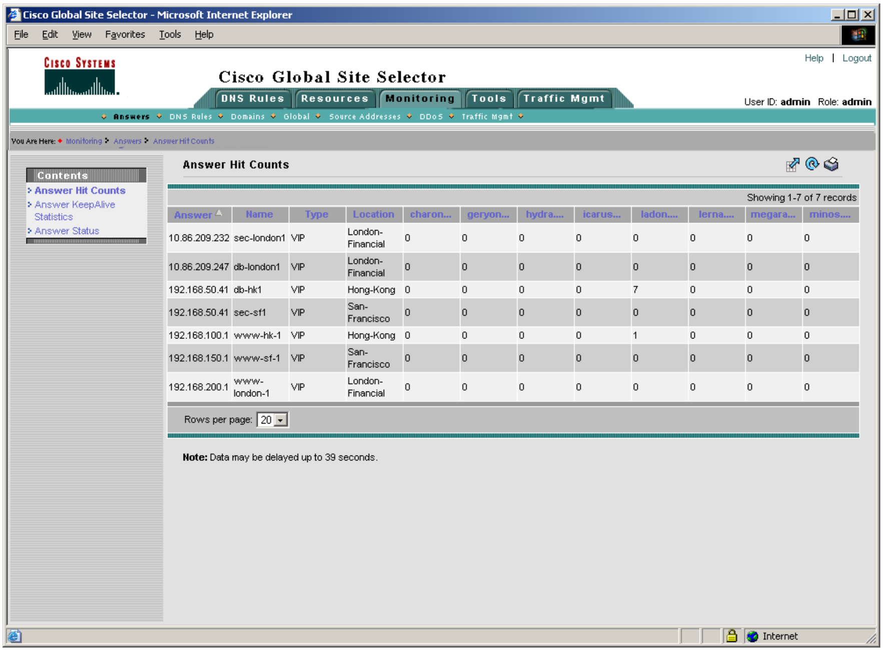
Monitoring Answer Hit Counts

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:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Answers** navigation link.
3. Click the **Answer Hit Counts** navigation link (located in the Contents list). The Answer Hit Counts list page appears (Figure 10-1).

Figure 10-1 Answer Hit Counts List Page



User ID: **admin** Role: **admin**

Answer Hit Counts

Showing 1-7 of 7 records

Answer	Name	Type	Location	charon...	geryon...	hydra....	icarus...	ladon....	lerna....	megara...	minos....
10.86.209.232	sec-london1	VIP	London-Financial	0	0	0	0	0	0	0	0
10.86.209.247	db-london1	VIP	London-Financial	0	0	0	0	0	0	0	0
192.168.50.41	db-hk1	VIP	Hong-Kong	0	0	0	0	7	0	0	0
192.168.50.41	sec-sf1	VIP	San-Francisco	0	0	0	0	0	0	0	0
192.168.100.1	www-hk-1	VIP	Hong-Kong	0	0	0	0	1	0	0	0
192.168.150.1	www-sf-1	VIP	San-Francisco	0	0	0	0	0	0	0	0
192.168.200.1	www-london-1	VIP	London-Financial	0	0	0	0	0	0	0	0

Rows per page: 20

Note: Data may be delayed up to 39 seconds.

Table 10-54 describes the fields on the Answer Hit Counts list page.

Table 10-54 Field Descriptions for Answer Hit Counts List Page

Field	Description
Answer	IP address of the answer resource
Name	Name assigned to the answer using the primary GSSM GUI
Type	Resources to which the GSS resolves DNS requests. The answer types include: VIP, CRA, or Name Server.
Location	GSS network location of the answer
Name of the GSS or GSSM	Number of requests directed to the answer by each GSS device

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

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.

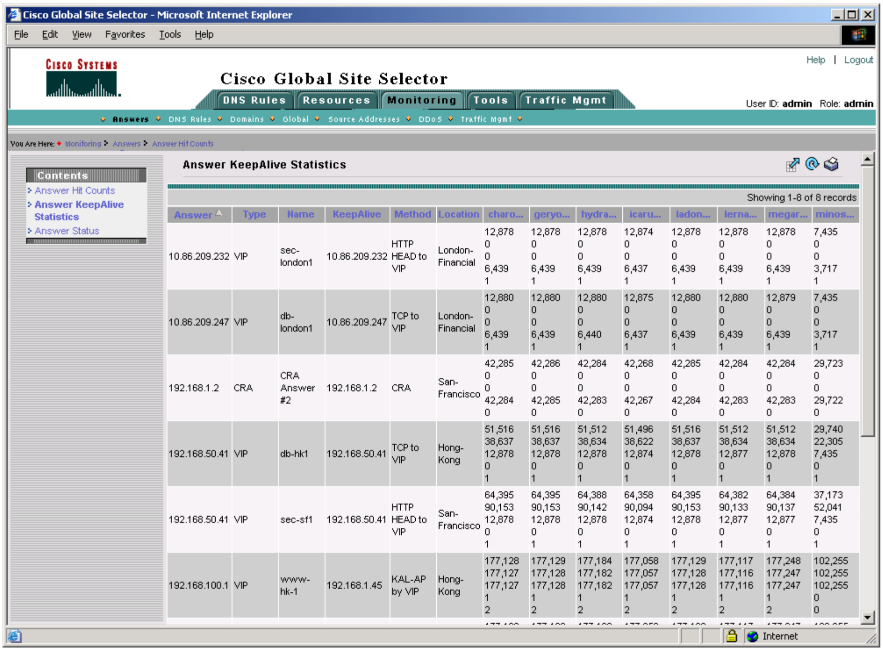
You may discover that certain answers may be offline or have problems staying online if a large number of keepalive probes are rejected or encounter transition conditions. Be aware also that when you use a TCP keepalive with the fast detection and graceful termination methods to test a Telnet service 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 three or four should prevent flapping on port 23 when connecting to a server running Windows Server 2003.

To view the keepalive statistics for each answer:

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 (Figure 10-2).

Figure 10-2 Answer Keepalive Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > Answers > Answer Hit Counts
Contents
Answer Hit Counts
Answer KeepAlive Statistics
Answer Status
Internet
240120

Answer KeepAlive Statistics

Showing 1-8 of 8 records

Answer	Type	Name	KeepAlive	Method	Location	charo...	geryo...	hydra...	icaru...	ladon...	lerna...	megar...	minos...
10.86.209.232	VIP	sec-london1	10.86.209.232	HTTP HEAD to VIP	London-Financial	12,878 0 0 6,439 1	12,878 0 0 6,439 1	12,878 0 0 6,439 1	12,874 0 0 6,437 1	12,878 0 0 6,439 1	12,878 0 0 6,439 1	12,878 0 0 6,439 1	7,435 0 0 3,717 1
10.86.209.247	VIP	db-london1	10.86.209.247	TCP to VIP	London-Financial	12,880 0 0 6,439 1	12,880 0 0 6,439 1	12,880 0 0 6,440 1	12,875 0 0 6,437 1	12,880 0 0 6,439 1	12,880 0 0 6,439 1	12,879 0 0 6,439 1	7,435 0 0 3,717 1
192.168.1.2	CRA	CRA Answer #2	192.168.1.2	CRA	San-Francisco	42,285 0 0 42,284 0	42,286 0 0 42,285 0	42,284 0 0 42,283 0	42,268 0 0 42,267 0	42,285 0 0 42,284 0	42,284 0 0 42,283 0	42,284 0 0 42,283 0	29,723 0 0 29,722 0
192.168.50.41	VIP	db-hk1	192.168.50.41	TCP to VIP	Hong-Kong	51,516 38,637 12,878 0 1	51,516 38,637 12,878 0 1	51,512 38,634 12,878 0 1	51,496 38,622 12,874 0 1	51,516 38,637 12,878 0 1	51,512 38,634 12,877 0 1	51,512 38,634 12,878 0 1	29,740 22,305 7,435 0 1
192.168.50.41	VIP	sec-sf1	192.168.50.41	HTTP HEAD to VIP	San-Francisco	64,395 90,153 12,878 0 1	64,395 90,153 12,878 0 1	64,388 90,142 12,878 0 1	64,358 90,094 12,874 0 1	64,395 90,153 12,878 0 1	64,382 90,133 12,877 0 1	64,384 90,137 12,877 0 1	37,173 52,041 7,435 0 1
192.168.100.1	VIP	www-hk-1	192.168.1.45	KAL-AP by VIP	Hong-Kong	177,128 177,127 177,127 1 2	177,129 177,128 177,128 1 2	177,184 177,182 177,182 1 2	177,058 177,057 177,057 1 2	177,129 177,128 177,128 1 2	177,117 177,116 177,116 1 2	177,248 177,247 177,247 1 2	102,255 102,255 102,255 0 0

Table 10-55 describes the fields on the Answer KeepAlive Statistics list page.

Table 10-55 Field Descriptions for Answer Keepalive Statistics List Page

Field	Description
Answer	IP address of the answer resource probed by the GSS.
Type	Resources to which the GSS resolves DNS requests. The answer types include: VIP, CRA, or Name Server.
Name	Name assigned to the answer using the primary GSSM GUI.
Keepalive	Address assigned to the remote device, CRA, or name server that the GSS is to forward requests.
Method	The keepalive method used by the answer: VIP (virtual IP address), NS (name server), or CRA (content routing agent)

Table 10-55 Field Descriptions for Answer Keepalive Statistics List Page (continued)

Field	Description
Location	GSS network location of the answer
Name of the GSS or GSSM	The number of keepalive probes directed to the answer by each GSS device, as well as the record of how those probes were handled. Statistics are presented in the following order: • **Keepalive packets sent**—Total number of keepalive probes sent to the answer by each GSS on the network • **Keepalive packets received**—Total number of keepalive probes returned from the answer • **Keepalive positive probe count**—Total number of keepalive probes received by the GSS to which a positive (OK) response was returned • **Keepalive negative probe count**—Total number of keepalive probes received by the GSS to which a negative response was returned • **Keepalive transition count**—Total number of keepalive probe transitions (for example, from the INIT to the ONLINE state) experienced by the keepalive

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

Monitoring Answer Status

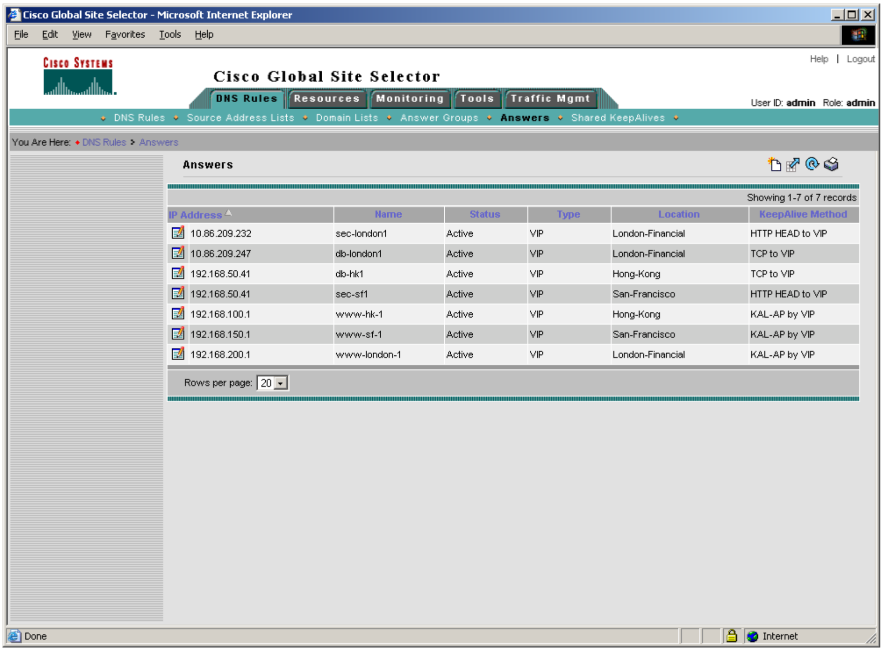
The Answer Status list page displays statistics about the GSS answer resources. Answers can be sorted by IP address, name, type, location, or online status according to a particular device.

To view the status of your GSS answers:

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 (Figure 10-3).

Figure 10-3 Answer Status List Page



Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Help | Logout
Cisco Systems
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
DNS Rules
Source Address Lists
Domain Lists
Answer Groups
Answers
Shared KeepAlives
You Are Here: DNS Rules > Answers
Answers
Done
Internet
240121

Showing 1-7 of 7 records

IP Address	Name	Status	Type	Location	KeepAlive Method
10.86.209.232	sec-london1	Active	VIP	London-Financial	HTTP HEAD to VIP
10.86.209.247	db-london1	Active	VIP	London-Financial	TCP to VIP
192.168.50.41	db-hk1	Active	VIP	Hong-Kong	TCP to VIP
192.168.50.41	sec-sf1	Active	VIP	San-Francisco	HTTP HEAD to VIP
192.168.100.1	www-hk-1	Active	VIP	Hong-Kong	KAL-AP by VIP
192.168.150.1	www-sf-1	Active	VIP	San-Francisco	KAL-AP by VIP
192.168.200.1	www-london-1	Active	VIP	London-Financial	KAL-AP by VIP

Rows per page: 20

Table 10-56 describes the fields on the Answer Status list page.

Table 10-56 Field Descriptions for Answer Status List Page

Field	Description
Answer	IP address of the answer resource
Name	Name assigned to the answer using the primary GSSMGUI
Type	Resources to which the GSS resolves DNS requests. The answer types include: VIP, CRA, or Name Server.
Location	GSS network location of the answer
Name of the GSS or GSSM	Online status of the answer according to the named device

4. Click the column header of any of the displayed columns to sort your answers by a particular property.

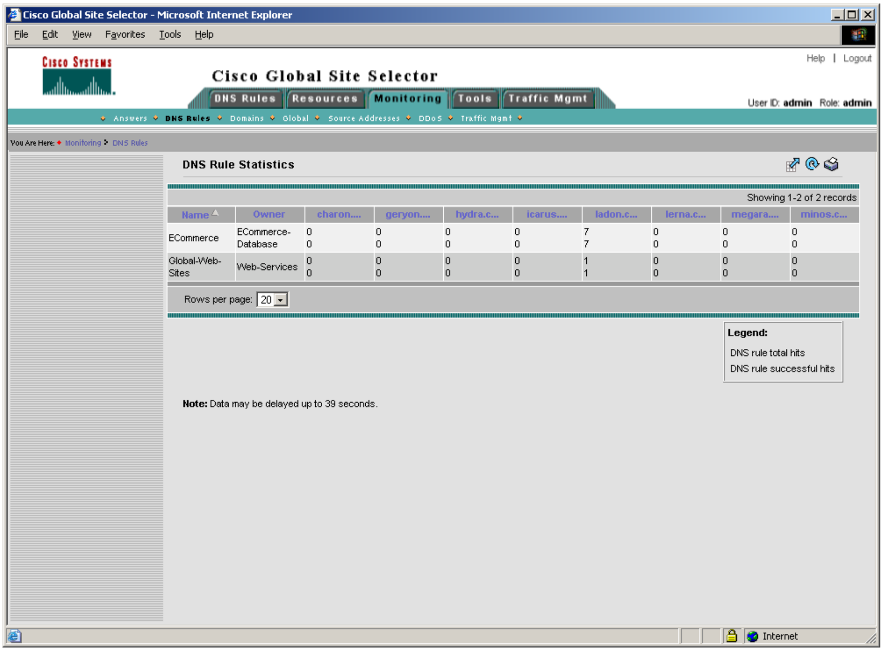
Monitoring DNS Rule Statistics

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:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **DNS Rules** navigation link. The DNS Rule Statistics list page appears (Figure 10-4).

Figure 10-4 DNS Rule Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring DNS Rules
Internet
240127

DNS Rule Statistics

Showing 1-2 of 2 records

Name	Owner	charon....	geryon....	hydra.c...	icarus....	ladon.c...	lerna.c...	megara....	minos.c...
ECommerce	ECommerce-Database	0 0	0 0	0 0	0 0	7 7	0 0	0 0	0 0
Global-Web-Sites	Web-Services	0 0	0 0	0 0	0 0	1 1	0 0	0 0	0 0

Rows per page: 20

Legend:
DNS rule total hits
DNS rule successful hits

Note: Data may be delayed up to 39 seconds.

Table 10-57 describes the fields on the DNS Rule Statistics list page.

Table 10-57 Field Descriptions for DNS Rule Statistics List Page

Field	Description
Name	Name assigned to the answer using the primary GSSM.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	Total hit count and successful hit count for the DNS rule from the listed GSS device. Refer to the legend that appears below the listed DNS rules for information about identifying which value represents total hits and which value represents successful DNS requests served.

3. Click the column header of any of the displayed columns to sort your DNS rules by a particular property.

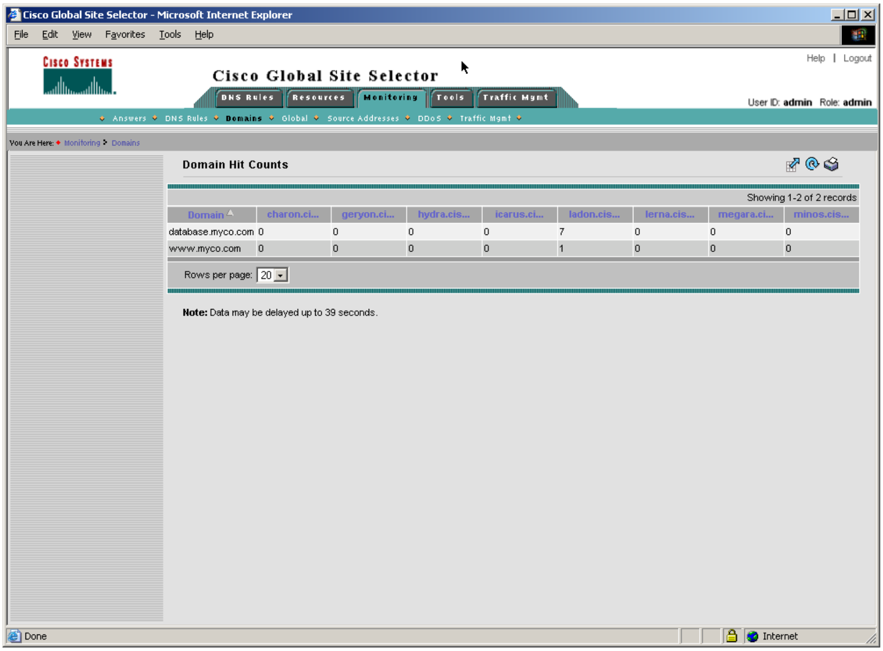
Monitoring Domain Hit Counts

The Domain Hot Counts list page displays statistics about the hosted domains that the GSS serves, as well as 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:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Domains** navigation link. The Domain Hit Counts list page appears (Figure 10-5).

Figure 10-5 Domain Hit Counts List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > Domains
Done
Internet
240128

Domain Hit Counts

Showing 1-2 of 2 records

Domain	charon.ci...	geryon.ci...	hydra.cis...	icarus.ci...	ladon.cis...	lerna.cis...	megara.ci...	minos.cis...
database.myco.com	0	0	0	0	7	0	0	0
www.myco.com	0	0	0	0	1	0	0	0

Rows per page: 20

Note: Data may be delayed up to 39 seconds.

Table 10-58 describes the fields on the Domain Hit Counts list page.

Table 10-58 Field Descriptions for Domain Hit Counts List Page

Field	Description
Domain	DNS domains that the GSS is responsible. These are the domains contained in your domain lists.
Name of the GSS or GSSM	Total number of requests for the listed domain from each GSS device

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

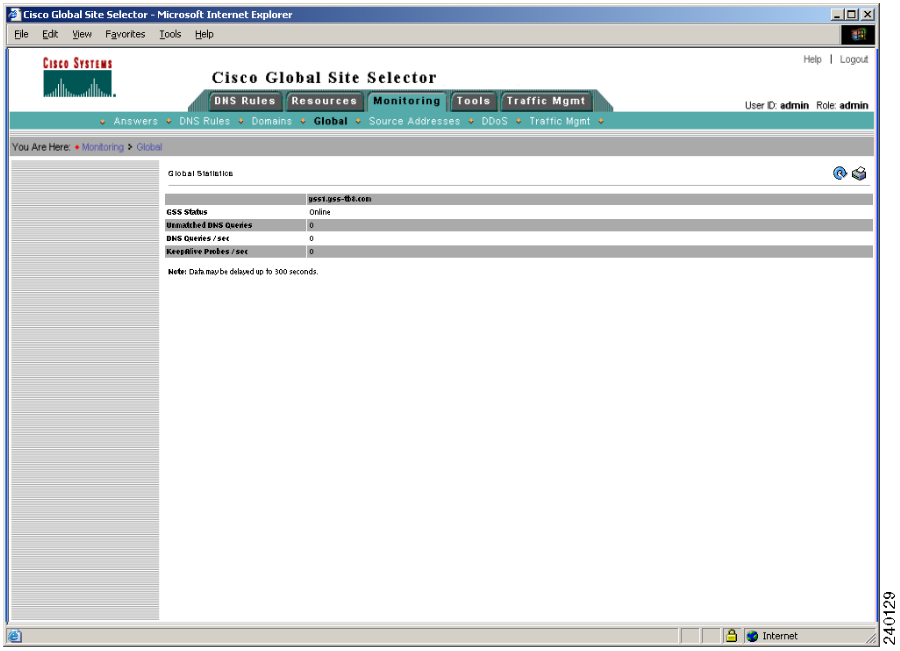
Monitoring Global Statistics

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, as well as the online status of each GSS device.

To view the status of your GSS network:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Global** navigation link. The Global Statistics list page (Figure 10-6) appears.

Figure 10-6 Global Statistics List Page



Global Statistics

	yss1.yss-tb8.com
GSS Status	Online
Unmatched DNS Queries	0
DNS Queries / sec	0
KeepAlive Probes / sec	0

Note: Data may be delayed up to 300 seconds.

Table 10-59 describes the fields on the Global Statistics list page.

Table 10-59 Field Descriptions for Global Statistics List Page

Field	Description
GSS Status	Online status of each GSS device in your GSS network
Unmatched DNS Queries	Total number of DNS queries received by each listed device for which no answer could be found
DNS Queries/sec	Average number of DNS queries received, per second, by each listed GSS device
Keepalive Probes/sec	Average number of keepalive probes received by each listed GSS device each second

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

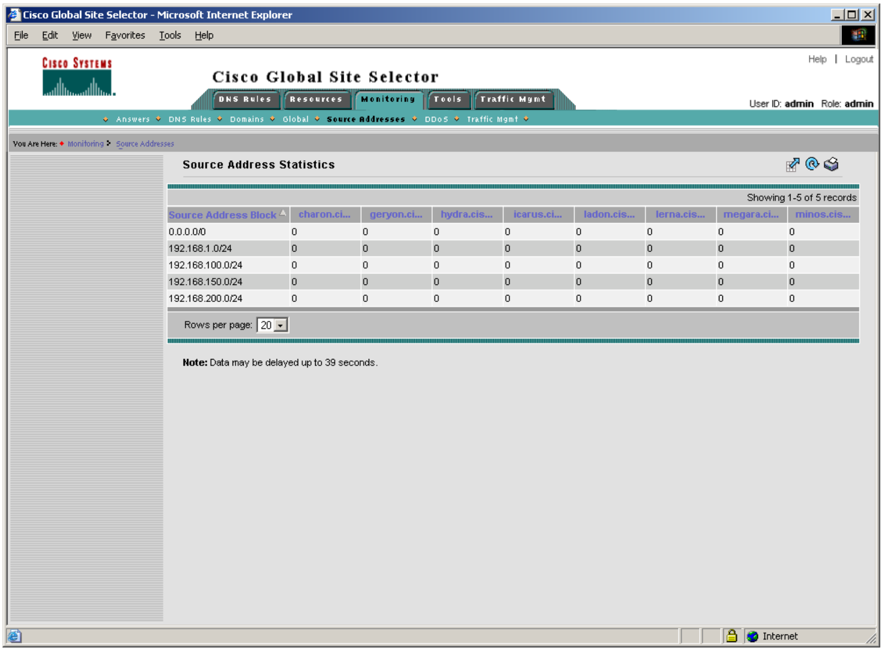
Monitoring Source Address Statistics

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:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **Source Addresses** navigation link. The Source Address Statistics list page appears (Figure 10-7).

Figure 10-7 Source Address Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Cisco Systems
Cisco Global Site Selector
Help | Logout
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Answers
DNS Rules
Domains
Global
Source Addresses
DDoS
Traffic Mgmt
You Are Here: Monitoring Source Addresses
Internet
240163

Source Address Statistics

Showing 1-5 of 5 records

Source Address Block	charon.ci...	geryon.ci...	hydra.cis...	icarus.ci...	ladon.cis...	lerna.cis...	megara.ci...	minos.cis...
0.0.0.0/0	0	0	0	0	0	0	0	0
192.168.1.0/24	0	0	0	0	0	0	0	0
192.168.100.0/24	0	0	0	0	0	0	0	0
192.168.150.0/24	0	0	0	0	0	0	0	0
192.168.200.0/24	0	0	0	0	0	0	0	0

Rows per page: 20

Note: Data may be delayed up to 39 seconds.

Table 10-60 describes the fields on the Source Address Statistics list page.

Table 10-60 Field Descriptions for Source Address Statistics List Page

Field	Description
Source Address Block	Address or range of addresses that originate the DNS queries. Source address blocks make up GSS source address lists.
Name of the GSS or GSSM	Total number of requests received by the listed GSS device from each source address or address block.

3. Click the column header of any of the displayed columns to sort the listed domains by a particular property.

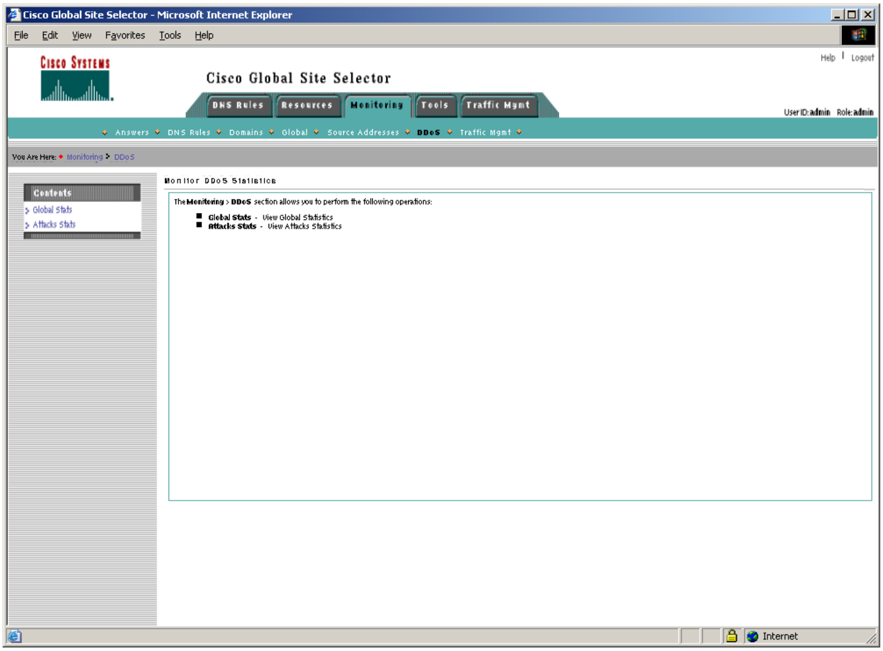
Monitoring DDoS Statistics

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:

1. From the primary GSSM GUI, click the **Monitoring** tab.
2. Click the **DDDoS** navigation link. The Monitor DDos Statistics page appears with two sub-menu items, Global Stats and Attack Stats (Figure 10-8).

Figure 10-8 Monitor DDoS Statistics Menu Page



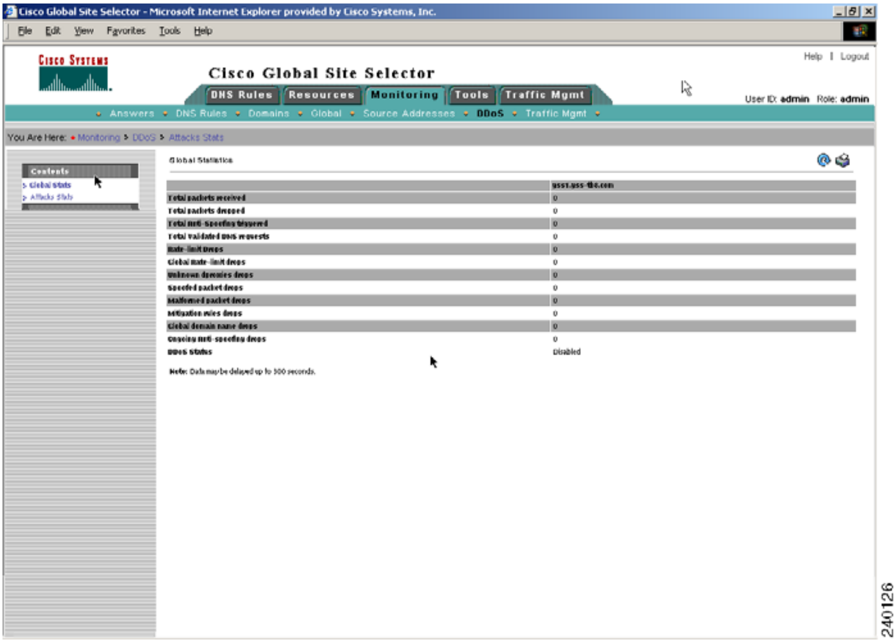
Monitor DDoS Statistics

The **Monitoring** > **DDoS** section allows you to perform the following operations:

- **Global Stats** - View Global Statistics
- **Attacks Stats** - View Attacks Statistics

3. Click the **Global Stats** selection to view the DDoS Global Statistics (Figure 10-9).

Figure 10-9 DDoS Global Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > DDoS > Attacks Stats
Contents
Global Stats
Attacks Stats
Global Statistics
240126

	gss1.gss-tbs.com
Total packets received	0
Total packets dropped	0
Total anti-spoofing triggered	0
Total validated DNS requests	0
Rate-limit Drops	0
Global rate-limit drops	0
Unknown domains drops	0
Spoofed packet drops	0
Malformed packet drops	0
Mitigation rules drops	0
Global domain name drops	0
Ongoing anti-spoofing drops	0
DDoS status	Disabled

Note: Data may be delayed up to 300 seconds.

Table 10-61 describes the fields on the Global Statistics list page.

Table 10-61 Field Descriptions for Global Statistics List Page

Field	Description
Total packets received	Packets received and handled by the GSS. The Total packets received counter is the sum of the legitimate counter and the malicious counter.
Total packets dropped	Packets that were identified by the GSS DDoS protection and mitigation functions as part of an attack and dropped.
Total Anti-Spoofing triggered	The total number of packets that triggered the GSS DDoS protection anti-spoofing function.

Table 10-61 Field Descriptions for Global Statistics List Page

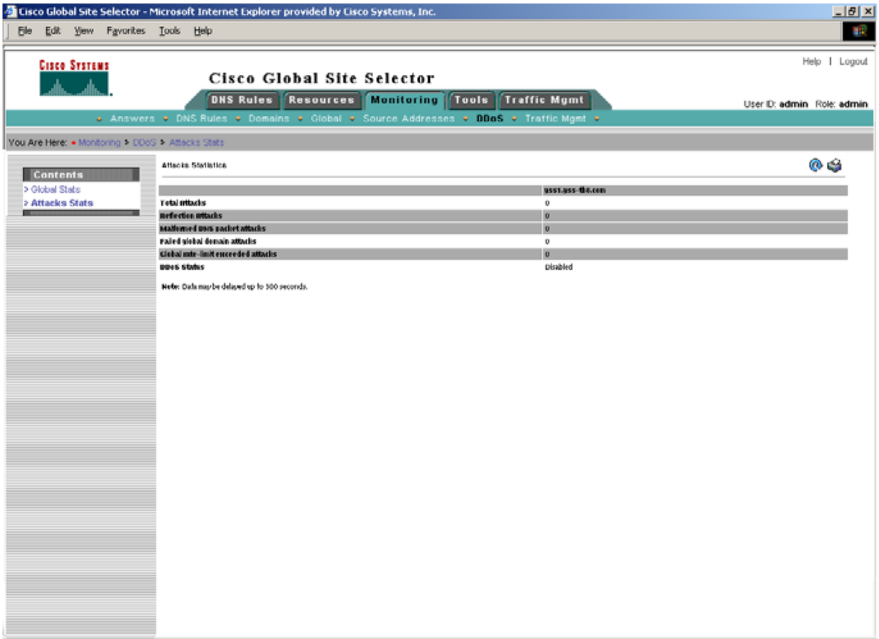
Field	Description
Total Validated DNS requests	The total number of packets that were successfully dropped by the GSS DDoS protection anti-spoofing function.
Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation rate-limiting functions as part of an attack and dropped. The rate limit is the maximum number of DNS requests the GSS can receive from the D-proxy per second.
Global Rate-limit drops	Packets that were identified by the GSS DDoS protection and mitigation global rate-limiting function as part of an attack and dropped.
Unknown dproxies drops	An D-proxy that has not been classified as spoofed or non-spoofed by the DDoS protection and mitigation function is unknown. The DDoS function starts anti-spoofing for an unknown D-proxy. If the number of packets from unknown D-Proxies exceeds the specified rate limit, the unknown drops start.
Spoofed packet drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an attack and dropped.
Malformed packet drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a malformed packet and dropped.
Mitigation rules drops	Packets that were identified by the GSS DDoS protection and mitigation functions as violating mitigation rules and dropped.
Global domain name drops	Packets that were identified by the GSS DDoS protection and mitigation functions as a global domain name and dropped.

Table 10-61 Field Descriptions for Global Statistics List Page

Field	Description
Ongoing anti-spoofing drops	Packets that were identified by the GSS DDoS protection and mitigation anti-spoofing functions as part of an ongoing attack and dropped.
DDoS Status	Specifies whether the DDoS detection and mitigation module has been enabled or disabled on the GSS.

4. Click the **Attack Stats** selection to view the DDoS Attack Statistics (Figure 10-10).

Figure 10-10 DDoS Attack Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules
Resources
Monitoring
Tools
Traffic Mgmt
User ID: admin Role: admin
Answers
DNS Rules
Domains
Global
Source Addresses
DDoS
Traffic Mgmt
You Are Here: Monitoring > DDoS > Attacks Stats
Contents
> Global Stats
> Attacks Stats
240125

Attacks Statistics

	gss1.gss-tb.com
Total attacks	0
Reflection attacks	0
Malformed DNS packet attacks	0
Failed global domain attacks	0
Global rate-limit exceeded attacks	0
DDoS status	Disabled

Note: Data may be delayed up to 300 seconds.

Table 10-62 describes the fields on the Attack Statistics list page.

Table 10-62 Field Descriptions for Attack Statistics List Page

Field	Description
Total attacks	Total number of DNS attacks detected by the GSS.
Reflection attacks	An 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.
Malformed DNS packet attacks	An attack in which the GSS is flooded with malformed DNS packets.
Failed global domain attacks	The failed domain counter provides a total for DNS queries that failed to match the global domain name.
Global rate-limit exceeded attacks	An attack in which the maximum number of DNS requests the GSS receives from the D-proxy per second exceeds the global limit.
DDoS status	Specifies whether the DDoS detection and mitigation module has been enabled or disabled on the GSS.

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 procedures:

- 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

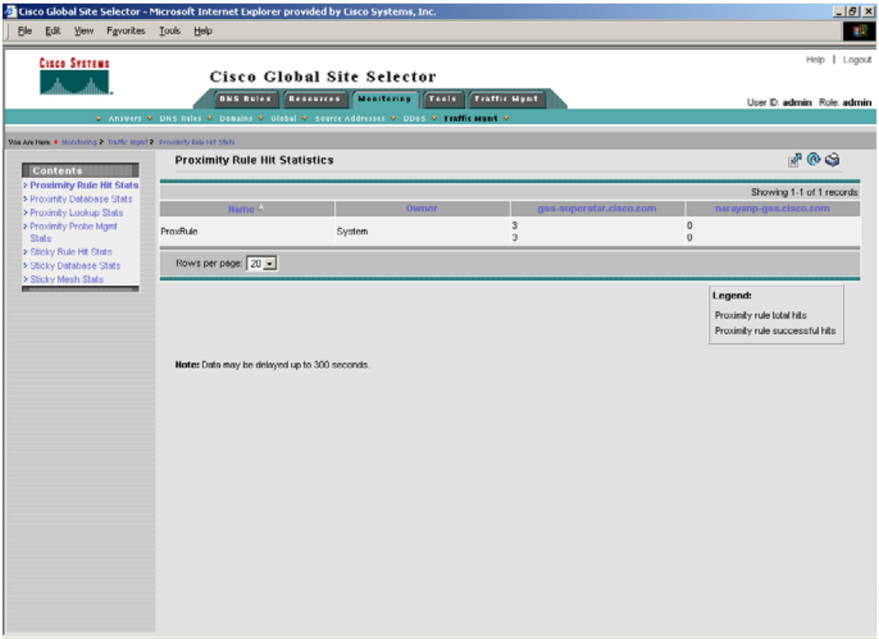
Monitoring Proximity Rule Hit Count Statistics

Use the Proximity Rule Hit Count Statistics list page to view 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:

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 (Figure 10-11).

Figure 10-11 Proximity Rule Hit Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > Traffic Mgmt > Proximity Rule Hit Stats
Contents
Proximity Rule Hit Stats
Proximity Database Stats
Proximity Lookup Stats
Proximity Probe Mgmt Stats
Sticky Rule Hit Stats
Sticky Database Stats
Sticky Mesh Stats
240159

Proximity Rule Hit Statistics

Showing 1-1 of 1 records

Name	Owner	gss-superstar.cisco.com	narayanp-gss.cisco.com
ProxRule	System	3 3	0 0

Rows per page: 20

Legend:
Proximity rule total hits
Proximity rule successful hits

Note: Data may be delayed up to 300 seconds.

Table 10-63 describes the fields on the Proximity Rule Hit Statistics list page.

Table 10-63 Field Descriptions for Proximity Rule Hit Statistics List Page

Field	Description
Name	Name of the matched DNS rule.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	For each GSS or GSSM: • The number of DNS requests that match the DNS rule. • The number of DNS responses successfully returned with a proximate answer for the DNS rule. Refer to the legend that appears below the listed DNS rules for information about identifying which value represents the proximity hit count and which value represents the number of successful matches.

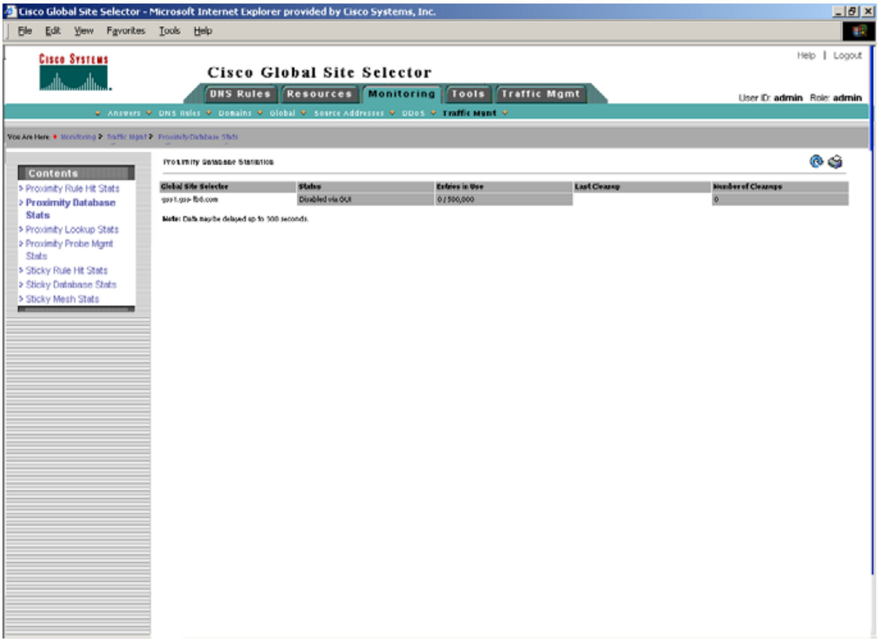
Monitoring Proximity Database Statistics

Use the Proximity Database Statistics list page to view 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:

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 (Figure 10-12).

Figure 10-12 Proximity Database Statistics List Page



Proximity Database Statistics

Global Site Selector	Status	Entries in Use	Last Cleanup	Number of Cleanups
gss1.gss-fb6.com	Disabled via GUI	0 / 500,000		0

Note: Data may be delayed up to 300 seconds.

Table 10-64 describes the fields on the Proximity Database Statistics list page.

Table 10-64 Field Descriptions for Proximity Database Statistics List Page

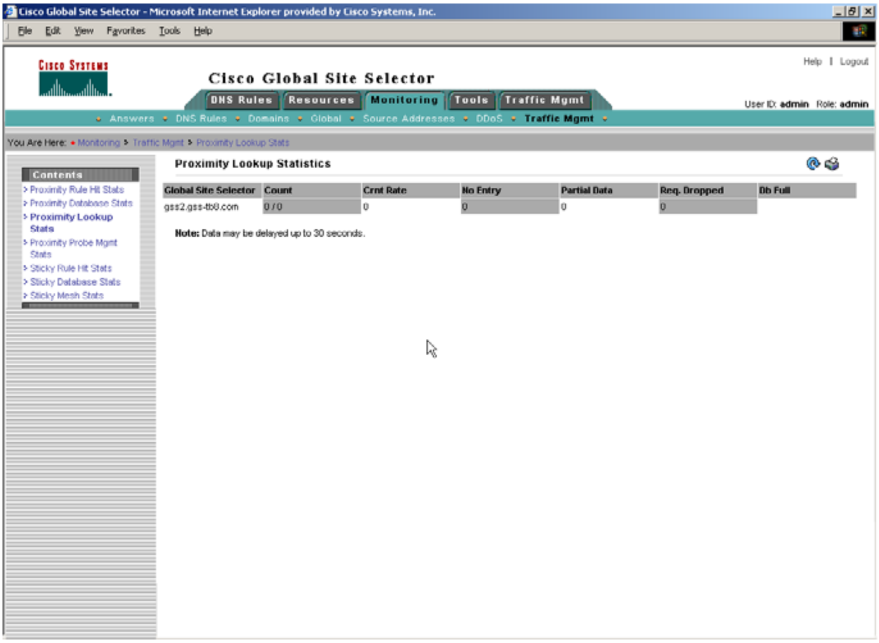
Field	Description
Global Site Selector	Name of the GSS or GSSM device
Entries in Use	Number of entries currently in the proximity database, out of a maximum of 500,000 entries
Last Cleanup	Last time the GSS removed the least recently used entries from the proximity database
Number of Cleanups	Number of entries removed during the cleanup process

Monitoring Proximity Lookup Statistics

Use the Proximity Lookup Statistics list page to view statistics about the number of entries in the proximity database:

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 (Figure 10-13).

Figure 10-13 Proximity Lookup Statistics List Page



Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > Traffic Mgmt > Proximity Lookup Stats
Contents
Proximity Rule Hit Stats
Proximity Database Stats
Proximity Lookup Stats
Proximity Probe Mgmt Stats
Sticky Rule Hit Stats
Sticky Database Stats
Sticky Mesh Stats
240156

Proximity Lookup Statistics

Global Site Selector	Count	Crnt Rate	No Entry	Partial Data	Req. Dropped	Db Full
gss2.gss-tb8.com	0 / 0	0	0	0	0	

Note: Data may be delayed up to 30 seconds.

Table 10-65 describes the fields on the Proximity Lookup Statistics list page.

Table 10-65 Field Descriptions for Proximity Lookup Statistics List Page

Field	Description
Global Site Selector	Name of the GSS or GSSM device
Count	Total number of proximity lookup requests made to the GSS
Crnt Rate	Current request rate per second that requests are made to the GSS to perform a proximity lookup in the database
No Entry	Number of times 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 the GSS was unable to perform a proximity add because the database exceeded the maximum number of entries

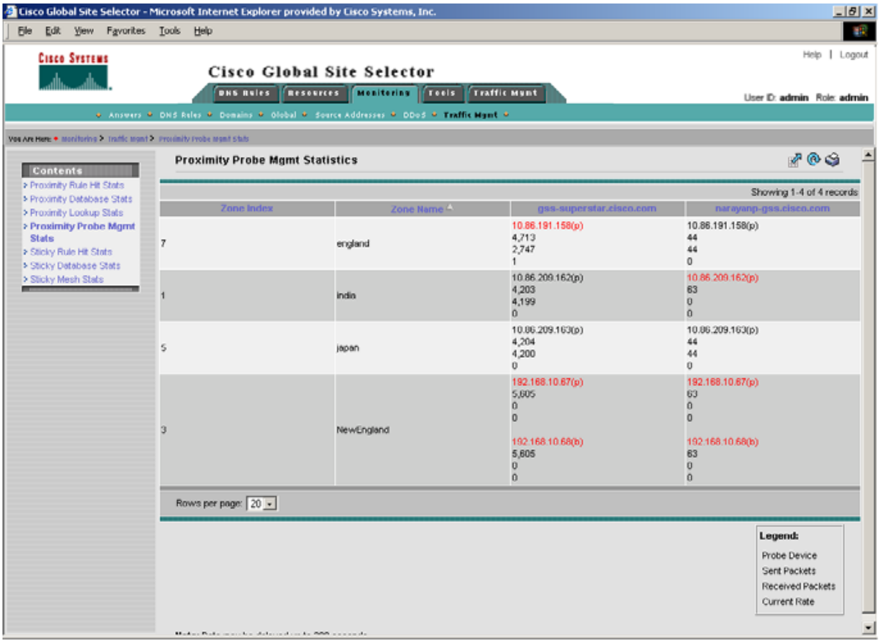
Monitoring Proximity Probe Management Statistics

Use the Proximity Probe Management Statistics list page to view statistics about the ICMP and TCP probes transmitted from the probing devices.

To view statistics about the probing requests and responses:

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 (Figure 10-14).

Figure 10-14 Proximity Probe Mgmt Statistics List Page



Proximity Probe Mgmt Statistics

Showing 1-4 of 4 records

Zone Index	Zone Name	gss-superstar.cisco.com	narayanp-gss.cisco.com
7	england	10.86.191.158(p) 4,713 2,747 1	10.86.191.158(p) 44 44 0
1	india	10.86.209.162(p) 4,203 4,199 0	10.86.209.162(p) 63 0 0
5	japan	10.86.209.163(p) 4,204 4,200 0	10.86.209.163(p) 44 44 0
3	NewEngland	192.168.10.67(p) 5,605 0 0 192.168.10.68(b) 5,605 0 0	192.168.10.67(p) 63 0 0 192.168.10.68(b) 63 0 0

Rows per page: 20

Legend:

Probe Device
Sent Packets
Received Packets
Current Rate

Table 10-66 describes the fields on the Proximity Probe Mgmt Statistics list page.

Table 10-66 Field Descriptions for Proximity Probe Mgmt Statistics List Page

Field	Description
Zone Index	The numerical identifier of the proximity zone.
Zone Name	The name of the proximity zone.
Name of the GSS or GSSM	For each GSS or GSSM: • The IP address of the probe device. • The total number of DRP echo and measurement packets sent by the GSS to the probing device in the proximity zone. • The total number of DRP echo and measurement packets received by the GSS from the probing device in the proximity zone. • The current packet send rate per second. Refer to the legend that appears below the listed zones for information about identifying which value represents sent echo and measurement packets, which value represents received echo and measurement packets, and which value represents the current packet send rate.

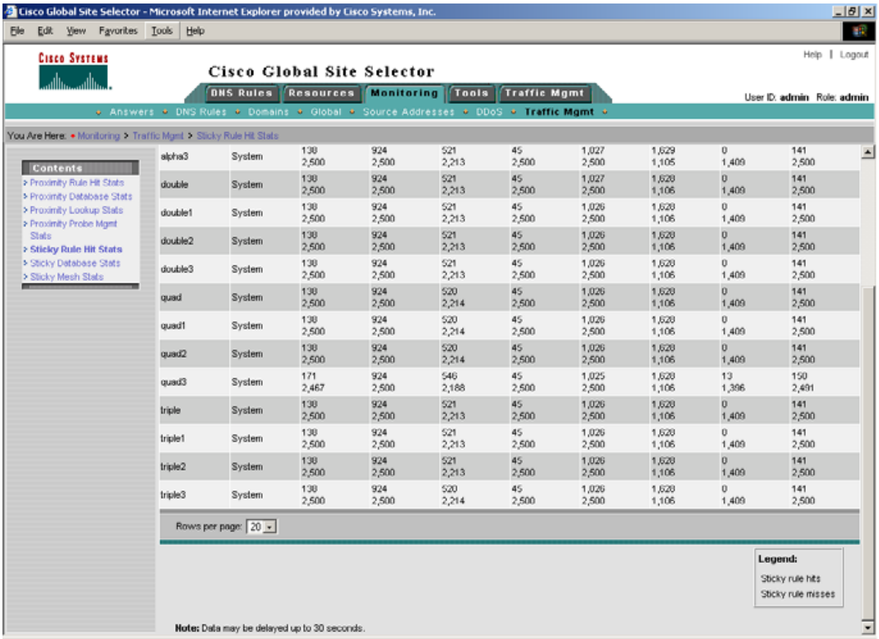
Monitoring Sticky Rule Hit Statistics

Use the Sticky Rule Hit Statistics list page to view 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:

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 (Figure 10-15).

Figure 10-15 Sticky Rule Hit Statistics List Page



alpha3	System	138 2,500	924 2,500	521 2,213	45 2,500	1,027 2,500	1,629 1,105	0 1,409	141 2,500
double	System	138 2,500	924 2,500	521 2,213	45 2,500	1,027 2,500	1,628 1,106	0 1,409	141 2,500
double1	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
double2	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
double3	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
quad	System	138 2,500	924 2,500	520 2,214	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
quad1	System	138 2,500	924 2,500	520 2,214	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
quad2	System	138 2,500	924 2,500	520 2,214	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
quad3	System	171 2,467	924 2,500	546 2,188	45 2,500	1,025 2,500	1,628 1,106	13 1,396	150 2,491
triple	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
triple1	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
triple2	System	138 2,500	924 2,500	521 2,213	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500
triple3	System	138 2,500	924 2,500	520 2,214	45 2,500	1,026 2,500	1,628 1,106	0 1,409	141 2,500

Rows per page: 20

Legend:
Sticky rule hits
Sticky rule misses

Note: Data may be delayed up to 30 seconds.

Table 10-67 describes the fields on the Sticky Rule Hit Statistics list page.

Table 10-67 Field Descriptions for Sticky Rule Hit Statistics List Page

Field	Description
Name	Name of the matched DNS rule.
Owner	GSS owner to whom the DNS rule has been assigned.
Name of the GSS or GSSM	For each GSS or GSSM: • The total number of successful sticky answer matches in the sticky database for the DNS rule. • The total number of failed sticky answer lookups in the sticky database for the DNS rule. Refer to the legend that appears below the listed DNS rules for information about identifying which value represents successful matches and which value represents failed lookups.

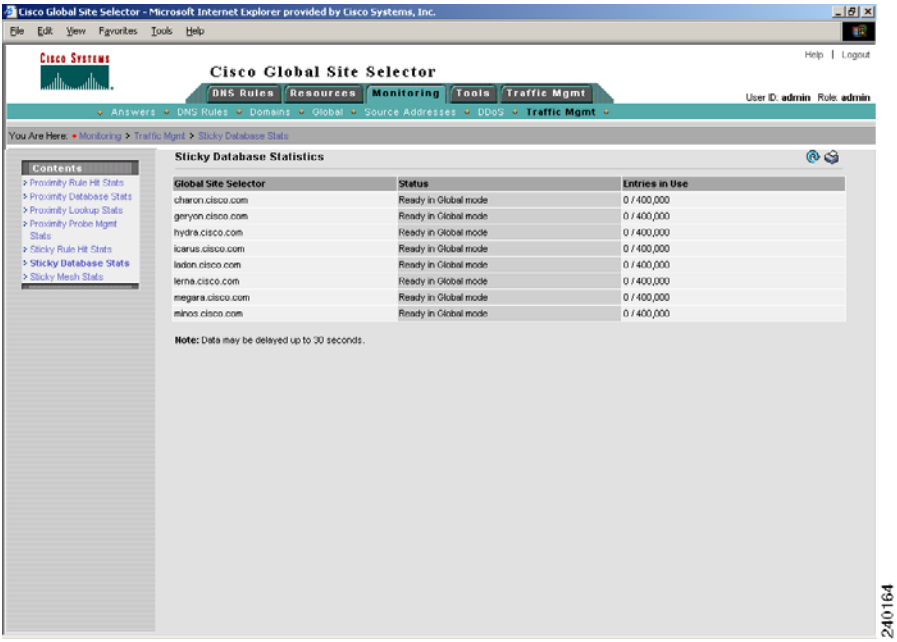
Monitoring Sticky Database Statistics

Use the Sticky Database Statistics list page to view the number of entries in the sticky database.

To view the number of entries in the sticky database:

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 (Figure 10-16).

Figure 10-16 Sticky Database Statistics List Page


Cisco Global Site Selector - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Help | Logout
Cisco Global Site Selector
DNS Rules Resources Monitoring Tools Traffic Mgmt
User ID: admin Role: admin
Answers DNS Rules Domains Global Source Addresses DDoS Traffic Mgmt
You Are Here: Monitoring > Traffic Mgmt > Sticky Database Stats
Contents
Proximity Rule Hit Stats
Proximity Database Stats
Proximity Lookup Stats
Proximity Probe Mgmt Stats
Sticky Rule Hit Stats
Sticky Database Stats
Sticky Mesh Stats
240164

Sticky Database Statistics

Global Site Selector	Status	Entries in Use
charon.cisco.com	Ready in Global mode	0 / 400,000
geryon.cisco.com	Ready in Global mode	0 / 400,000
hydra.cisco.com	Ready in Global mode	0 / 400,000
icarus.cisco.com	Ready in Global mode	0 / 400,000
ladon.cisco.com	Ready in Global mode	0 / 400,000
lerna.cisco.com	Ready in Global mode	0 / 400,000
megara.cisco.com	Ready in Global mode	0 / 400,000
minos.cisco.com	Ready in Global mode	0 / 400,000

Note: Data may be delayed up to 30 seconds.

Table 10-68 describes the fields on the Sticky Database Statistics list page.

Table 10-68 Field Descriptions for Sticky Database Statistics List Page

Field	Description
Global Site Selector	Name of the GSS device (GSSM or GSS).
Status	Sticky status of the named device and sticky mode. Status conditions can include Disabled, Local, Global, and Stopped.
Entries in Use	Number of entries currently in the sticky database out of a maximum of 400,000 entries.

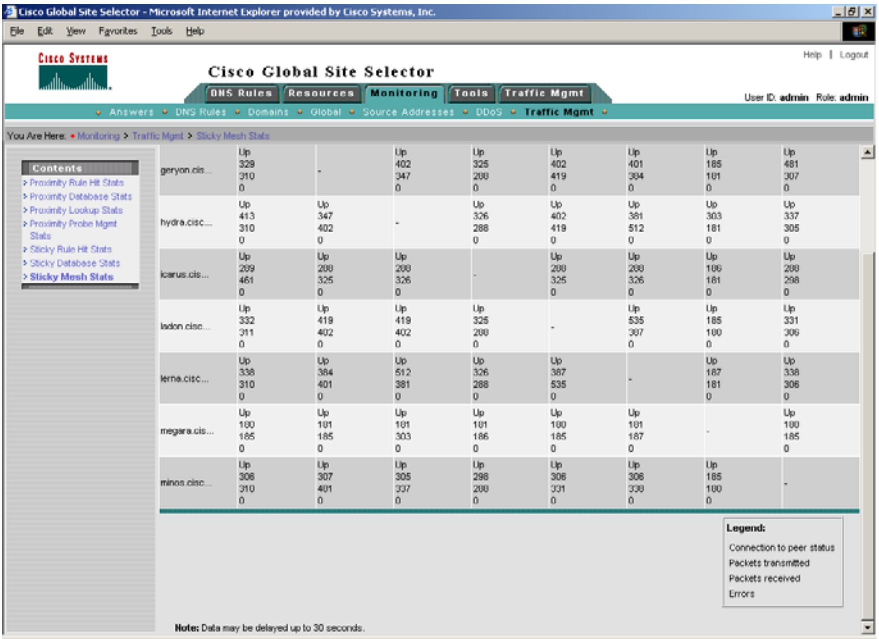
Monitoring Global Sticky Mesh Statistics

Use the Sticky Mesh Statistics list page to display 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:

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 (Figure 10-17).

Figure 10-17 Sticky Mesh Stats List Page



geryon.cis...	Up 329 310 0	-	Up 402 347 0	Up 325 200 0	Up 402 419 0	Up 401 384 0	Up 185 181 0	Up 481 307 0
hydra.cisc...	Up 413 310 0	Up 347 402 0	-	Up 326 288 0	Up 402 419 0	Up 381 512 0	Up 303 181 0	Up 337 305 0
icarus.cis...	Up 209 461 0	Up 200 325 0	Up 200 326 0	-	Up 200 325 0	Up 200 326 0	Up 186 181 0	Up 200 298 0
ladon.cisc...	Up 332 311 0	Up 419 402 0	Up 419 402 0	Up 325 200 0	-	Up 535 387 0	Up 185 180 0	Up 331 306 0
lerna.cisc...	Up 338 310 0	Up 384 401 0	Up 512 381 0	Up 326 288 0	Up 387 535 0	-	Up 187 181 0	Up 338 306 0
megara.cis...	Up 180 185 0	Up 181 185 0	Up 181 303 0	Up 181 186 0	Up 180 185 0	Up 181 187 0	-	Up 180 185 0
minos.cisc...	Up 306 310 0	Up 307 401 0	Up 305 337 0	Up 298 200 0	Up 306 331 0	Up 306 338 0	Up 185 180 0	-

Legend:
Connection to peer status
Packets transmitted
Packets received
Errors

Note: Data may be delayed up to 30 seconds.

Table 10-69 describes the fields on the Sticky Mesh Statistics list page.

Table 10-69 Field Descriptions for Sticky Mesh Statistics List Page

Field	Description
GSS/Peer	Name of the GSS device (GSSM or GSS) in the mesh along with its peers.
Name of the GSS or GSSM in the mesh	For each GSS peer in the mesh, each column lists the following statistics: • **Connection to peer status**—Online status of each peer in the mesh. The possible states are Stopped, Init, Opened, Authentication, Up, and Down. • **Packets transmitted**—Number of packets transmitted from the GSS or GSSM to each peer in the mesh. • **Packets received**—Number of packets received by the GSS or GSSM from each peer in the mesh. • **Down Events**—The number of down events encountered for the session between the peers in the mesh. Refer to the legend that appears below the listed peer GSS or GSSM in the mesh for information about identifying which statistic represents the online peer status, packets transmitted, packets received, and session down events.

APPENDIX A

Primary GSSM Global Server Load-Balancing Error Messages

This appendix describes error messages that you may encounter when using the primary GSSM GUI to perform global server load balancing. Error messages are organized by primary GSSM GUI components.

This chapter contains the following major sections:

- Answer Error Messages
- Answer Group Error Messages
- Domain List Error Messages
- DNS Rule Error Messages
- KeepAlive Error Messages
- Location Error Messages
- Network Error Messages
- Owner Error Messages
- Proximity Error Messages
- Region Error Messages
- Source Address List Error Messages
- Sticky Error Messages
- User Account Error Messages
- User Views Error Messages

Answer Error Messages

Table A-1 lists the potential error messages that may appear when configuring answers.

Table A-1 Answer Error Messages

Error Message	Description	Recommended Action
`Invalid answer name. If entered, name must not be the empty string.`	You entered an invalid name for the answer. Answer names cannot be blank or contain blank spaces.	Enter a valid alphanumeric answer name of a least 1 and no more than 80 characters in length that does not contain spaces.
`Invalid answer name. Name length must not exceed 80 characters.`	You entered an answer name that contains too many characters.	Enter a valid alphanumeric answer name of at least 1 and no more than 80 characters in length that does not contain spaces.
`Invalid CRA timing decay. Timing decay must be between 1 and 10.`	You entered an invalid number for the CRA timing decay.	Enter a number between 1 and 10. Lower timing decay values mean that more recent DNS races are weighted more heavily than older races. Higher decay values mean that the results of older races are weighted more heavily than more recent races.
`Invalid CRA static RTT value. Static RTT must be between 0 and 1000.`	You entered an invalid number for the static round-trip time (RTT). This is a manually entered value that is used by the GSS to represent the time it takes for traffic to reach and return from a host.	Enter a static RTT value between 0 and 1000.
`A` *`VIP/Name Server/CRA`*`-type answer named` *`answer_name`* `already exists. If specified, name and type must uniquely identify an answer.`	You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and answer type.	Assign a new name or answer type to your answer to make it unique.

Table A-1 Answer Error Messages (continued)

Error Message	Description	Recommended Action
`An unnamed` *`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.`	You attempted to create an answer that already exists on the GSS. You cannot have two answers with the same name and IP address.	Assign a new name to your answer to make it unique.
`The maximum number of` *`number VIP/Name Server/CRA`*`-type answers has been met.`	You attempted to create an answer when the maximum number of that type of answer has already been created.	Remove an existing answer of the same type.
`CRA decay value must be specified.`	You attempted to create a CRA answer type without specifying a decay value. The decay value is required to tell the GSS how to evaluate and weigh DNS race results.	Enter a number between 1 and 10 for the CRA decay, with 1 causing the GSS to weigh recent DNS race results more heavily, and 10 telling it to weigh them less heavily.
`CRA static RTT must be specified.`	You attempted to create a CRA answer type without specifying a static round-trip time (RTT) value. The RTT value is used to force the GSS to use a value that you supply as the round-trip time necessary to reach the requesting D-proxy.	Enter a number between 1 and 1000 for the CRA round-trip time in milliseconds.
`Invalid keepalive tag. Tag must be at least one character in length.`	You attempted to create a VIP answer with a KAL-AP By Tag keepalive, but you have not specified a value for the tag in the field provided.	Enter an alphanumeric tag between 1 and 76 characters in the Tag field.
`Invalid keepalive tag. Tag length must not exceed 76 characters.`	You attempted to create a VIP answer with a KAL-AP By Tag keepalive, but you have specified a value for the tag that contains too many characters.	Enter an alphanumeric tag between 1 and 76 characters in the Tag field.

Table A-1 Answer Error Messages (continued)

Error Message	Description	Recommended Action
`NS-type answer` *`IP Address`* `has the same IP address as GSS` *`GSS_name`*`. GSS IP addresses must not equal any NS-type answers.`	You attempted to create a name server answer type with the same IP address as a GSS device on the same GSS network. Name server answers cannot use the same address as GSS devices belonging to the same GSS network.	Assign a valid IP address to your name server answer.
`Invalid answer order. Order must not be negative.`	You attempted to assign a negative order number to your answer. The order must be a positive number.	Enter a nonnegative whole number for the order.

Answer Group Error Messages

Table A-2 lists the potential error messages that may appear when configuring answer groups.

Table A-2 Answer Group Error Messages

Error Message	Description	Recommended Action
`This answer group cannot be deleted because it is referenced by` *`number`* `DNS rule balance clause(s).`	You attempted to delete an answer group that is being referenced by one or more DNS rules.	Modify any DNS rules that are referencing the answer group so that those rules do not point to the group, and then try again to delete the group.
`Invalid answer group name. Name must be entered.`	You attempted to create an answer group without assigning a name to that group. All answer groups must have names of at least one character.	Enter a name for the new answer group in the field provided, and then click **Save**.

Table A-2 Answer Group Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid answer group name. Name length must not exceed 80 characters.`	You attempted to assign the answer group an invalid name.	Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
`Invalid answer group name. Name must not contain spaces.`	You attempted to assign the answer group an invalid name.	Enter an alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
`An answer group named` *`name`* `already exists. Name must uniquely identify an answer group.`	You attempted to assign the answer group a name that is already being used by a different GSS device.	Enter a unique alphanumeric name for the answer group that is fewer than 80 characters and does not contain spaces.
`The maximum number of` *`number`* `answers per` *`VIP/Name Server/CRA`*`-type group has been met.`	You attempted to add an answer to an answer group to which the maximum number of answers has already been assigned.	Remove an answer from the group, or add the answer to a group to which the maximum number of answers has not already been added.
`Invalid answer load threshold. Load threshold must be between 2 and 254.`	You attempted to assign an invalid load threshold to your answer in the LT field.	Assign a load threshold for the answer that is between 2 and 254 in the LT field.

Domain List Error Messages

Table A-3 lists the potential error messages that may appear when configuring domain lists.

Table A-3 Domain List Error Messages

Error Message	Description	Recommended Action
`<domain name> must contain at least one character.`	You attempted to add a domain to a domain list with an invalid name. Domains in domain lists must have names of at least one character.	Enter a name that is between 1 and 100 characters and then save your domain list.
`<domain name> character limit exceeded.`	You attempted to add a domain to a domain list using a name that is too long. Domains in domain lists cannot have names of more than 100 characters.	Enter a new domain name of no more than 100 characters and then save your domain list.
`Domain specification must not exceed 128 characters.`	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 longer than 128 characters.	Replace the domain with a domain name containing fewer than 128 characters and then save your domain list.
`<domain name> must not contain spaces.`	You attempted to add a domain to your domain list with a name that contains spaces. Domains in domain lists cannot have names that contain spaces.	Modify the domain name so that it does not contain spaces and then save your domain list.
`<domain name> is not a valid regular expression: <regular expression syntax error message here>`	You attempted to add a domain name to a domain list with a name that contains invalid characters or formatting. Domain names in domain lists must be valid regular expressions.	Modify the domain name so that it is a valid regular expression and does not contain any invalid characters or formatting. For example, www.cisco.com or .*\.cisco\.com, and then save your domain list.

Table A-3 Domain List Error Messages (continued)

Error Message	Description	Recommended Action
`<domain name> must not begin or end with '.'`	You attempted to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of the domain name.	Modify the domain name so that it does not contain a period at the beginning or end of the name and then save your domain list.
`<domain name> component must not begin or end with '-'`	You attempted to add a domain to a domain list with a literal name that contains an invalid character at the beginning or end of one component of the domain name. For example, www.cisco-.com.	Modify the domain name so that it does not contain a dash (-) at the beginning or end of any segment of the name and then save your domain list.
`<domain name> contains invalid character '<character>' (<ASCII value of the character>)`	You attempted to add a domain to a domain list with a name that contains an invalid text character. Domains belonging to domain lists must have names that are regular expressions.	Modify the domain name so that it does not contain an invalid text character and then save your domain list.
`This domain list cannot be deleted because it is referenced by X DNS rule`	You attempted to delete a domain list that is being referenced by one or more DNS rules.	Modify any DNS rules that use the domain list so that they no longer reference it and then try again to delete the list.
`Invalid domain list name. Name must be entered.`	You attempted to create a domain list without a name. Domain lists must have names of at least one character.	Assign a name of at least 1 and no more than 80 characters to your domain list and then save it.
`Invalid domain list name. Name length must not exceed 80 characters.`	You attempted to create a domain list with a name that is too long.	Assign a name of at least 1 and no more than 80 characters to your domain list and then save it.

Table A-3 Domain List Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid domain list name. Name must not contain spaces.`	You attempted to create a domain list with a name that contains spaces. Domain list names cannot contain spaces.	Assign a name without spaces to your domain list. Names must consist of at least 1 and no more than 80 characters. Save your domain list when you have assigned it a valid name.
`A domain list named '<name>' already exists. Name must uniquely identify a domain list.`	You attempted to assign a name to your domain list that has already been assigned to another domain list on the same GSS network.	Assign a unique name to your new domain list and then save the list.
`The maximum number of <limit> domains per list has been met.`	You attempted to add a domain to your domain list when the maximum number of domains has already been added to that list.	Remove an existing domain from the domain list and then add the new domain. Alternatively, create a domain list to hold the new domain and any subsequent domains that you wish to add.

DNS Rule Error Messages

Table A-4 lists the potential error messages that may appear when configuring DNS rules.

Table A-4 DNS Rules Error Messages

Error Message	Description	Recommended Action
`TTL must be specified for balance method associated with CRA- or VIP-type answer group.`	You attempted to create a balance clause without specifying a Time To Live (TTL) for answers returned by the clause.	Enter a TTL value between 0 and 604,800 seconds.
`Invalid balance clause TTL. TTL must be between 0 and 604,800.`	You attempted to create a balance clause with an incorrect TTL value for answers provided by the balance clause.	Enter a TTL value between 0 and 604,800 seconds.
`Invalid balance clause position. Position must be between 0 and 2.`	You attempted to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.	Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order, with no gaps between them.
`Hash type must be specified for answer group using hash balance method.`	You attempted to create an answer group using the balance method “Hashed” with the selected answer, but you have not selected one (or more) hash methods: By Domain Name and By Source Address.	Select one or more of the available hash methods by checking the box corresponding to the methods that you wish to use with this balance clause.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
`Balance clause boomerang fragment size must be specified.`	You attempted to create a balance clause using the boomerang balance method but have not specified a fragment size in the Fragment Size field. The fragment size determines the preferred size of the boomerang race response that is produced by a match to a DNS rule and is sent to the requesting client.	Enter a fragment size between 28 and 1980 in the field provided. The fragment size must be divisible by 4.
`Invalid balance clause Boomerang fragment size. Boomerang fragment size must be 0 or between 28 and 1980.`	You attempted to specify an unacceptable fragment size for this balance clause in the Fragment Size field.	Enter a valid fragment size. Fragment sizes must be between 28 and 1980 and must be divisible by 4.
`Invalid balance clause Boomerang fragment size. Boomerang fragment size must be a multiple of 4.`	You attempted to specify a fragment for this boomerang balance clause that is within the acceptable range but not divisible by 4. Fragment sizes must be divisible by 4.	Enter a fragment size between 28 and 1980 that is also divisible by 4. Zero is also an acceptable fragment size.
`Balance clause Boomerang IP TTL value must be specified.`	You attempted to create a balance clause using the boomerang balance method but have not specified an IP Time To Live (TTL) in the field provided. The IP TTL specifies the maximum number of network hops that can be used when returning a response to a CRA from a match on a DNS rule.	Enter an IP TTL between 1 and 255 in the field provided and then click **Save**.
`Invalid balance clause Boomerang IP TTL. Boomerang IP TTL must be between 1 and 255.`	You attempted to create a balance clause using the boomerang balance method but have specified an invalid IP Time to Live (TTL).	Enter an IP TTL between 1 and 255 in the field provided and then click **Save**.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
`Balance clause Boomerang maximum propagation delay must be specified.`	You attempted to create a balance clause using the boomerang balance method but have not specified a maximum propagation delay (Max Prop. Delay) in the field provided. The maximum propagation delay specifies the maximum length of time (in milliseconds) that is observed before the GSS forwards a Domain Name System (DNS) request to a content routing agent (CRA).	Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.
`Invalid balance clause Boomerang maximum propagation delay. Boomerang maximum propagation delay must be between 1 and 1000.`	You attempted to create a balance clause using the boomerang balance method but have not specified a valid maximum propagation delay (Max Prop. Delay) in the field provided.	Enter a maximum propagation delay between 1 and 1000 milliseconds in the Max Prop. Delay field.
`Balance clause Boomerang padding size must be specified.`	You attempted to create a balance clause using the boomerang balance method but have not specified a pad size in the Pad Size field. The pad size is the amount of extra data (in bytes) included with each content routing agent (CRA) response packet and is used to evaluate CRA bandwidth as well as latency when routing decisions are made.	Enter a valid pad size between 0 and 2000 in the Pad Size field.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid balance clause Boomerang padding size. Boomerang padding size must be between 0 and 2000.`	You attempted to create a balance clause using the boomerang balance method but have specified an invalid pad size in the Pad Size field.	Enter a valid pad size between 0 and 2000 in the Pad Size field.
`Invalid balance clause Boomerang secret. If specified, Boomerang secret must be between 1 and 64 characters in length.`	You attempted to create a balance clause using the boomerang balance method but have specified an invalid secret in the Secret field. The boomerang secret is a text string consisting of between 1 and 64 characters that is used to encrypt critical data sent between the boomerang server and content routing agents (CRAs). This key must be the same for each configured CRA.	Enter a valid boomerang secret between 1 and 64 characters in the Secret field.
`Balance clause Boomerang server delay must be specified.`	You attempted to create a balance clause using the boomerang balance method but have not specified a server delay in the Server Delay field. The boomerang server delay is the maximum delay (in milliseconds) that is observed before the boomerang server component of the GSS forwards the address of its “last gasp” server as a response to the requesting name server.	Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.
`Invalid balance clause Boomerang server delay. Boomerang server delay must be between 32 and 999.`	You attempted to create a balance clause using the boomerang balance method but have specified an invalid server delay in the Server Delay field.	Enter a valid server delay between 32 and 999 milliseconds in the Server Delay field.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid DNS rule name. Name must be entered.`	You attempted to create a DNS rule without assigning a name to the rule. DNS rules must have names of between 1 and 100 characters.	Assign a name to your DNS rule using the Rule Name field and then try again to save the rule.
`Invalid DNS rule name. Name length must not exceed 100 characters.`	You attempted to assign a name to your DNS rule that is too long. The maximum length for DNS rules is 100 characters.	Enter a name for your DNS rule that is between 1 and 100 characters and then attempt to save the rule again.
`Invalid DNS rule name. Name must not contain spaces.`	You attempted to assign your DNS rule a name that contains spaces.	Enter a valid name for your DNS rule that is between 1 and 100 characters and does not contain spaces.
`A DNS rule using the specified source address list, domain list, and matching query type already exists. Source address list, domain list, and matching query type must uniquely identify a DNS rule.`	You attempted to create a DNS rule that already exists. DNS rules must specify a unique combination of source address list, domain list, and matching query type.	Reconfigure your DNS rule so that it does not exactly match the preexisting rule and then save the rule.
`Duplicate answer group/balance method assignment detected. A DNS rule cannot use the same answer group and balance method in multiple balance clauses.`	You attempted to create two identical answer group and balance method clauses in your DNS rule. Each clause must use a unique combination of answer groups and balance methods.	Modify one of your answer group and balance method pairs so that it is no longer identical to the other and then save your DNS rule.

Table A-4 DNS Rules Error Messages (continued)

Error Message	Description	Recommended Action
`Balance clause gap detected at position {0,1,2}. Balance clauses must be specified sequentially without gaps.`	You attempted to create a clause for your DNS rule that is out of sequence. The DNS Rule Builder provides options for three balance clauses, which must be created in order, with no gaps between clauses. For example, if you are using only one balance clause, it must appear in the first position. It cannot be listed in the second or third positions with the first position left blank.	Rearrange your balance clauses in the DNS Rule Builder so that they are listed in the proper order, with no gaps between them.
`A DNS rule named` *`DNS_Rule_name`* `already exists. Name must uniquely identify a DNS rule.`	You attempted to assign a name to the DNS rule that is already assigned to another rule. DNS rule names must be unique.	Assign the rule a name that is not already being used and then save the rule.
`Balance clause 1/2 cannot be sticky because clause number 0/1 is not sticky.`	You attempted to enable sticky on Balance Clause 2 without first enabling sticky on Balance Clause 1. The GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction is also true if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.	Enable sticky for Balance Clause 1 before enabling sticky for Balance Clause 2, and, if necessary, enable sticky for Balance Clause 2 before enabling sticky for Balance Clause 3.
`Invalid balance method. Proximity can not be enabled for balance method Hashed.`	You attempted to specify the hashed balance method for an answer group in a balance clause that has proximity enabled. The GSS does not support proximity in a DNS rule with the hashed balance method.	Choose a different balance method for the answer group from the Select Balance Method drop-down list.

KeepAlive Error Messages

Table A-5 lists the potential error messages that may appear when configuring keepalives.

Table A-5 Keepalive Error Messages

Error Message	Description	Recommended Action
`Invalid CAPP hash secret. Secret must be entered.`	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have not specified a secret in the field provided.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
`Invalid CAPP hash secret. Secret length must not exceed 31 characters.`	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
`Invalid HTTP HEAD response timeout.`	You attempted to specify an HTTP HEAD response timeout that is invalid.	Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.
`Response timeout must be between 20 and 60 seconds.`	You attempted to specify an HTTP HEAD response timeout that is invalid.	Enter a response timeout between 20 and 60 seconds in the HTTP HEAD response timeout field of the Shared Keepalive details page.
`Invalid HTTP HEAD destination port. Destination port must be between 1 and 65,535.`	You attempted to specify a port number for HTTP HEAD traffic that is invalid.	In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.

Table A-5 Keepalive Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid HTTP HEAD path. Path length must not exceed 256 characters.`	You attempted to specify an HTTP HEAD path that is not valid.	Enter a valid path shorter than 256 characters in the HTTP HEAD default path field in the Shared Keepalive details page.
`Invalid <keepalive type> minimum probe frequency. Frequency must be between <min> and <max>.`	You attempted to specify a minimum probe interval for your keepalive type that is invalid.	Specify an interval (in seconds) within the range specified for that keepalive type in the Shared Keepalive details page. The interval range for the CRA keepalive type is between 1 and 60 seconds. For all other keepalive types, it is between 45 and 255 seconds.
`Duplicate keepalive address detected. A keepalive must not be configured to use the same primary and secondary addresses.`	You attempted to configure a KAL-AP keepalive that is identical to a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a different primary and secondary address.
`Duplicate keepalive primary address '<primaryaddress>' detected. An address can be used by at most one KAL-AP type keepalive.`	You attempted to configure a KAL-AP keepalive that uses the same primary IP address as a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a primary IP address that is not already being used by another keepalive.
`Duplicate keepalive secondary address '<secondary address>' detected. An address can be used by at most one KAL-AP type keepalive.`	You attempted to configure a KAL-AP keepalive that uses the same secondary IP address as a keepalive of the same type that already exists.	Configure the KAL-AP keepalive to use a secondary IP address that is not already being used by another keepalive.
`HEAD Duplicate keepalive detected. An HTTP HEAD keepalive must not use the same address, destination path, host tag, and port as another HTTP HEAD keepalive.`	You attempted to configure an HTTP HEAD keepalive that features an identical configuration to that of another HTTP HEAD keepalive on your GSS network.	Configure the HTTP HEAD keepalive to use a unique configuration of address, destination path, host tag, and port.

Table A-5 Keepalive Error Messages (continued)

Error Message	Description	Recommended Action
`Duplicate keepalive detected. An ICMP keepalive must not use the same address as another ICMP keepalive.`	You attempted to configure an ICMP keepalive with an IP address that is identical to that of another ICMP keepalive on your GSS network.	Configure the ICMP to use a unique IP address.
`Invalid CAPP hash secret. Secret length must not exceed 31 characters.`	You attempted to create a KAL-AP keepalive using a CAPP hash secret but have specified a secret that is too long.	Enter a CAPP hash secret of no more than 31 characters in the field provided.
`Invalid HTTP HEAD destination port. If specified, destination port must be between 0 and 65,535.`	You attempted to specify a port number for HTTP HEAD traffic that is invalid.	In the HTTP HEAD destination port field in the Shared Keepalive details page, enter a port number between 1 and 65,535 through which HTTP HEAD keepalive traffic will pass. The default port is 80.
`Invalid HTTP HEAD host tag. Host tag length must not exceed 128 characters.`	You attempted to create an HTTP HEAD host tag that is too long.	Enter an HTTP HEAD host tag of no more than 128 characters.

Location Error Messages

Table A-6 lists the potential error messages that may appear when configuring locations.

Table A-6 Locations Error Messages

Error Message	Description	Recommended Action
`The location is still being referenced by other objects and cannot be removed.`	You attempted to delete a location that has answers or GSS devices associated with it.	Dissociate any answers or GSS devices from the location and then try again to delete it.
`There already exists a location named <name> in region <region> with the same name. Please specify a different location name.`	You attempted to create a location within this region when another location with the same name already exists.	Change the name of the location so that it is unique for the region.

Network Error Messages

Table A-7 lists the potential error messages that may appear when configuring the primary GSSM network.

Table A-7 Primary GSSM Network Error Messages

Error Message	Description	Recommended Action
`Maximum number of GSSMs exceeded. A GSS network can contain at most 2 GSSMs.`	You attempted to enable a GSSM when there are already two GSSMs enabled on your GSS network.	If necessary, remove your standby GSSM from your GSS network and then try again to enable the GSSM.
`The maximum number of <size> <className> has been met.`	You attempted to add a resource to your GSS network when the maximum number of that resource already exists.	Remove an existing resource of the same type and then try again to add the new resource.

Owner Error Messages

Table A-8 lists the potential error messages that may appear when configuring owners.

Table A-8 Owners Error Messages

Error Message	Description	Recommended Action
`Invalid owner name. Name must be entered.`	You attempted to create an owner without assigning the owner a name.	Owners must have a unique name. Enter a name for the owner in the field provided and then save the owner.
`Invalid owner name. Name length must not exceed 80 characters.`	You attempted to assign a name to an owner that is too long.	Assign your owner a name that is no longer than 80 characters.
`An owner named <owner name> already exists. Name must uniquely identify an owner.`	You attempted to assign your owner a name that is already assigned to another owner on your GSS network.	Assign a unique name to your owner.

Proximity Error Messages

Table A-9 lists the potential error messages that may appear when configuring network proximity.

Table A-9 Proximity Error Messages

Error Message	Description	Recommended Action
`Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.`	You entered an incorrect global subnet mask in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a valid host or network subnet mask. Be sure to enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit count notation (for example, /24).

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid Equivalence window. Equivalence window must be between 0 and 100`	You entered an incorrect Equivalence Window value in the the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter an equivalence window value from 0 to 100 percent to specify a percentage value that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. The default value is 20 percent.
`Invalid Entry inactivity timeout. Entry inactivity timeout must be between 15 and 10080`	You entered an incorrect Entry Inactivity Timeout value in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a value from 15 to 10080 minutes, specified in 5 minute intervals (15, 20, 25, 30, up to 10080), to configure the maximum time interval that can pass without the GSS receiving a lookup request for a proximity database entry before the GSS removes that entry. The default value is 60 minutes.
`Invalid Refresh probe interval. Refresh probe interval must be between 1 and 72`	You entered an incorrect Refresh Probe Interval value in the Global Proximity Configuration details page (Traffic Mgmt tab).	Enter a value from 1 to 72 hours to specify the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. The default value is 8 hours.
`Invalid Acceptable RTT. Acceptable RTT must be between 50 and 500`	You entered an incorrect acceptable RTT value in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.	Enter an acceptable RTT value from 50 to 500 ms to specify the value that the GSS uses as an acceptable RTT value when determining the most proximate answer. The default value is 100 ms.

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid Acceptable percentage of available zones. Acceptable percentage of available zones must be between 3 and 100`	You entered an incorrect proximity acceptable zone percentage in either the Global Proximity Configuration details page (Traffic Mgmt tab) or the DNS Rules Builder.	Enter a percentage of zones from 3 to 100 percent to specify a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The default value is 40 percent.
`Invalid DRP key. Key must have an Id.`	You attempted to create a DRP key without an ID value in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a key identification number from 0 to 255 to specify the ID value used by the GSS. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
`Invalid DRP key. Key must have a string.`	You attempted to create a DRP key without a string in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. Note that the first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
`Invalid key ID. Key with the ID 'xxx' already exists.`	You attempted to create a DRP key that is using an existing DRP key ID.	Specify a DRP key with a different ID in the Creating New DRP Key details page. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The range of key identification numbers is from 0 to 255.

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid DRP Key Id. DRP Key Id must be between 0 and 255.`	You entered an incorrect DRP key ID in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a key identification number from 0 to 255 to specify the ID value used by the GSS. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
`Invalid DRP Key String Length. DRP Key String Length must be between 1 and 80.`	You entered an incorrect DRP key string in the Creating New DRP Key details page (Traffic Mgmt tab).	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. Note that the first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
`Invalid key String. Key String cannot start with a digit.`	You attempted to create a DRP key that begins with a number.	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. Note that the first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.
`Invalid key String. Key String is limited to alphanumeric characters.`	You attempted to create a DRP key with non-supported characters.	Enter a string containing from 1 to 80 uppercase and lowercase alphanumeric characters. Note that the first character cannot be a number. The DRP string must be the same between the DRP agent on the Cisco IOS-based router and the GSS.

Table A-9 Proximity Error Messages (continued)

Error Message	Description	Recommended Action
`The maximum of 32 DRP Key has been met.`	The primary GSSM GUI supports a maximum of 32 keys.	If necessary, delete one or more DRP authentication keys from the primary GSSM GUI (see Chapter 9, Configuring Network Proximity).
`Invalid Zone Index. Zone Index must be between 1 and 32.`	You entered an incorrect proximity zone index in the Creating New Zone details page (Traffic Mgmt tab).	Enter an integer from 1 to 32 for the proximity zone Index. There is no default.
`Invalid zone name. Zone with index 'xxx' already has the name 'yyy'.`	You attempted to create a proximity zone that is using an existing zone name.	Enter a different description of the proximity zone. Only alphanumeric characters and the underscore ("_") character are allowed.
`Invalid zone index. Zone with the name 'yyy' already has index 'xxx'.`	You attempted to create a proximity zone that is using an existing index.	Enter a different proximity zone index. Enter an integer from 1 to 32. There is no default.
`The maximum of 32 Zones has been met.`	The primary GSSM GUI supports a maximum of 32 proximity zones.	If necessary, delete one or more proximity zones from the primary GSSM GUI (see Chapter 9, Configuring Network Proximity).
`Invalid probe device address. A probe device with address '1.2.3.4' already exists.`	You attempted to create a proximity zone that is using an existing IP address.	In the Probe Device field or the Backup Probe Device field of the Creating New Zone details page (depending on which field generated the error message), enter the correct IP address for the probe device servicing this zone.

Region Error Messages

Table A-10 lists the potential error messages that may appear when configuring regions.

Table A-10 Regions Error Messages

Error Message	Description	Recommended Action
`The region is still being referenced by other objects and cannot be removed.`	You attempted to delete a region that is associated with GSSs on your GSS network.	Disassociate the GSSs from the region and then try again to delete the region.
`There already exists a region named <region name>. All region names have to be unique.`	You attempted to assign a name to the region that is already being used by another region on your GSS network.	Assign a unique name to your region.

Source Address List Error Messages

Table A-11 lists the potential error messages that may appear when configuring source addresses.

Table A-11 Source Address List Error Messages

Error Message	Description	Recommended Action
`Invalid source address block '<block string>'. Address block must specify a host or a network.`	You attempted to specify an invalid source address range.	Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.
`Invalid source address block '<blockstring>'.  Address block must specify a class A, B, or C host or network.`	You attempted to specify an invalid source address range.	Enter a valid source address or block of source addresses. Source addresses cannot specify a multicast address list.
`Invalid source address list name. Name must be entered.`	You attempted to create a source address list without assigning the list a name.	Enter a name for the source address list in the Name field.

Table A-11 Source Address List Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid source address list name. Name length must not exceed 80 characters.`	You attempted to create a source address list with a name that is too long.	Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.
`Invalid source address list name. Name must not contain spaces.`	You attempted to create a source address list with a name that contains spaces. Source address list names cannot contain spaces.	Enter a valid name for the source address list that has fewer than 80 characters and does not contain spaces.
`This source address list cannot be deleted because it is referenced by <number> DNS rules.`	You attempted to delete a source address list that is referenced by one or more DNS rules.	Disassociate your DNS rules from the source address list using the DNS Rule Builder or DNS Rule Wizard and then attempt to delete the source address list again.
`A source address list named '<name>' already exists. Name must uniquely identify a source address list.`	You attempted to create a source address list using a name that is already being used by another source address list on your GSS network.	Assign a unique name to your source address list that is no more than 80 characters and does not contain spaces.
`The maximum number of 30 source address blocks per list has been met.`	You attempted to add a source address block to the source address list, when the maximum of 30 source address blocks has already been added to the list.	Remove an existing source address block, or create a source address list for the source address block that you wish to add.

Sticky Error Messages

Table A-12 lists the potential error messages that may appear when configuring DNS sticky.

Table A-12 Sticky Error Messages

Error Message	Description	Recommended Action
`Mask: Invalid value 255.255.abc.1. Please enter mask using proper format.`	You entered an incorrect global subnet mask in the Global Proximity Configuration details page.	Enter a valid host or network subnet mask. Be sure to enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit count notation (for example, /24).
`Invalid Sticky inactivity timeout. Sticky inactivity timeout must be between 15 and 10080.`	You entered an incorrect Entry Inactivity Timeout value in either the Global Sticky Configuration details page or in the DNS Rules Builder	Enter a value from 15 to 10080 minutes, specified in 5 minute intervals (15, 20, 25, 30, up to 10080), to configure the maximum time interval the maximum time period that an unused answer remains valid in the sticky database. The default value is 60 minutes.

Table A-12 Sticky Error Messages (continued)

Error Message	Description	Recommended Action
`Invalid Sticky inactivity timeout. Sticky inactivity timeout must be a multiple of 5.`	You entered an incorrect Entry Inactivity Timeout value in either the Global Sticky Configuration details page or in the DNS Rules Builder	Enter a value from 15 to 10080 minutes, specified in 5 minute intervals (15, 20, 25, 30, up to 10080), to configure the maximum time interval the maximum time period that an unused answer remains valid in the sticky database. The default value is 60 minutes.
`Invalid encryption string. Its length must not exceed 32 characters.`	You entered an incorrect encryption string in the Global Sticky Configuration details page (Traffic Mgmt tab).	Enter an unquoted text string with a maximum of 32 characters and no spaces as the encryption string used to authenticate communication between GSS peers in the mesh to prevent unauthorized device access.

User Account Error Messages

Table A-13 lists the potential error messages that may appear when configuring a user account.

Table A-13 Primary GSSM User Account Error Messages

Error Message	Description	Recommended Action
`There already exists a user account named <user name>. All user accounts must have a unique username.`	You attempted to create a user account with a name identical to that of an existing account.	Assign your new user account a unique name. See the *Cisco Global Site Selector Administration Guide* for details.
`You cannot delete the account with username 'admin'. This account must exist.`	You attempted to delete the administrator user account.	The primary GSSM GUI restricts you from deleting the administrator account. See the *Cisco Global Site Selector Administration Guide* for details.

User Views Error Messages

Table A-14 lists the potential error messages that may appear when creating a user view.

Table A-14 Primary GSSM User Views Error Messages

Error Message	Description	Recommended Action
`This view cannot be deleted because it is referenced by [number] user(s).`	You attempted to delete a user view that is assigned to one or more user accounts.	Access the Modifying User details page and change the assigned view to View All. See the *Cisco Global Site Selector Administration Guide* for details.
`Invalid view name. Name must be entered.`	You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the *Cisco Global Site Selector Administration Guide* for details.
`Invalid view name. Name length must not exceed 80 characters.`	You entered an incorrect view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the *Cisco Global Site Selector Administration Guide* for details.
`A view named [name] already exists. Name must uniquely identify a view.`	You entered a duplicate view name in the Create User Views details page or the Modify User Views details page.	Enter a valid view name. View names can be from 1 to 80 alphanumeric characters and cannot contain spaces. See the *Cisco Global Site Selector Administration Guide* for details.
`The maximum number of 500 owners per view has been met.`	The primary GSSM GUI supports a maximum of 500 owners in a custom user view.	If necessary, delete one or more owners previously assigned to the custom view. See the *Cisco Global Site Selector Administration Guide* for details.

Table A-14 Primary GSSM User Views Error Messages (continued)

Error Message	Description	Recommended Action
`The maximum number of 1000 locations per view has been met.`	The primary GSSM GUI supports a maximum of 1000 locations in a custom user view.	If necessary, delete one or more locations previously assigned to the custom view. See the *Cisco Global Site Selector Administration Guide* for details.
`The maximum number of 100 answers per view has been met.`	The primary GSSM GUI supports a maximum of 100 answers in a custom user view.	If necessary, delete one or more answers previously assigned to the custom view. See the *Cisco Global Site Selector Administration Guide* for details.
`The maximum number of 100 keepaives per view has been met.`	The primary GSSM GUI supports a maximum of 100 keepalives in a custom user view.	If necessary, delete one or more keepalives previously assigned to the custom view. See the *Cisco Global Site Selector Administration Guide* for details.

APPENDIX B

Sticky and Proximity XML Schema Files

This appendix describes how you can use the two XML schema files, included with the GSS, to describe and validate the sticky XML and proximity XML output files.

This chapter contains the following sections:

- Sticky XML Schema File Contents
- Proximity XML Schema File Contents

Sticky 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 the same directory where each XML output file resides.

Sticky XML Schema File Contents

The following document identifies the contents of the sticky XML schema, stickySchema.xsd:

```
<xsd:schema xmlns="http://www.cisco.com/gss/sticky"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            targetNamespace="http://www.cisco.com/gss/sticky"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified">

  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Cisco GSS Sticky Database
    </xsd:documentation>
  </xsd:annotation>

  <xsd:element name="Sticky_Database" type="StickyDatabaseType"/>
  <xsd:element name="Header" type="HeaderType"/>
  <xsd:element name="Source_Entries" type="SourceEntriesType"/>
  <xsd:element name="Source_Entry" type="SourceEntryType"/>
  <xsd:element name="Group_Entries" type="GroupEntriesType"/>
  <xsd:element name="Group_Entry" type="GroupEntryType"/>

  <xsd:complexType name="StickyDatabaseType">
    <xsd:sequence>
      <xsd:element ref="Header" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="Source_Entries" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="Source_Entry_Count" type="xsd:integer"
                   minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="Group_Entries" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="Group_Entry_Count" type="xsd:integer"
                   minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="HeaderType">
  <xsd:sequence>
    <xsd:element name="Version" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Time_Stamp" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Entry_Count" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Mask" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SourceEntriesType">
  <xsd:sequence minOccurs="0" maxOccurs="unbounded">
    <xsd:element ref="Source_Entry" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="GroupEntriesType">
  <xsd:sequence minOccurs="0" maxOccurs="unbounded">
    <xsd:element ref="Group_Entry" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SourceEntryType">
  <xsd:sequence>
    <xsd:element name="IP" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="D" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="R" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="A" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="H" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="T" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="GroupEntryType">
  <xsd:sequence>
    <xsd:choice minOccurs="1" maxOccurs="1">
```

```
        <xsd:element name="N" type="xsd:string"
                     minOccurs="1" maxOccurs="1"/>
        <xsd:element name="G" type="xsd:integer"
                     minOccurs="1" maxOccurs="1"/>
      </xsd:choice>
      <xsd:element name="D" type="xsd:string"
                   minOccurs="1" maxOccurs="1"/>
      <xsd:element name="R" type="xsd:string"
                   minOccurs="1" maxOccurs="1"/>
      <xsd:element name="A" type="xsd:string"
                   minOccurs="1" maxOccurs="1"/>
       <xsd:element name="H" type="xsd:integer"
                   minOccurs="1" maxOccurs="1"/>
      <xsd:element name="T" type="xsd:integer"
                   minOccurs="1" maxOccurs="1"/>
   </xsd:sequence>
  </xsd:complexType>

</xsd:schema>
```

Proximity XML Schema File Contents

The following document identifies the contents of the proximity XML schema, proximitySchema.xsd:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Cisco GSS Proximity Database
    </xsd:documentation>
  </xsd:annotation>

  <xsd:element name="ProximityDatabase" type="ProximityDatabaseType"/>
  <xsd:element name="Header" type="HeaderType"/>
  <xsd:element name="Entry" type="EntryType"/>
  <xsd:element name="ProbeTarget" type="ProbeTargetType"/>
  <xsd:element name="Zone" type="ZoneType"/>

  <xsd:complexType name="ProximityDatabaseType">
    <xsd:sequence>
      <xsd:element ref="Header" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="Entry" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
```

```
<xsd:complexType name="HeaderType">
  <xsd:sequence>
    <xsd:element name="Version" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Time_Stamp" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="EntryCount" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="EntryType">
  <xsd:sequence>
    <xsd:element name="EntryID" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="ModificationTimeStamp" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Static" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="DirectProbingInProgress" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="HitTimeStamp" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="HitCount" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element ref="ProbeTarget" minOccurs="1" maxOccurs="1"/>
    <xsd:element ref="Zone" minOccurs="32" maxOccurs="32"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ProbeTargetType">
  <xsd:sequence>
    <xsd:element name="IP" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Method" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="Type" type="xsd:string"
                 minOccurs="1" maxOccurs="1"/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ZoneType">
  <xsd:sequence>
     <xsd:element name="ID" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
    <xsd:element name="RTT" type="xsd:integer"
                 minOccurs="1" maxOccurs="1"/>
```

```
      <xsd:element name="RefreshTime" type="xsd:integer"
                   minOccurs="1" maxOccurs="1"/>
   </xsd:sequence>
  </xsd:complexType>

  <xsd:simpleType name="StaticType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="true"/>
      <xsd:enumeration value="false"/>
    </xsd:restriction>
</xsd:simpleType>

  <xsd:simpleType name="MethodType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="TCP"/>
      <xsd:enumeration value="ICMP"/>
      <xsd:enumeration value="NotUsed"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="TypeOfType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="static"/>
      <xsd:enumeration value="non-static"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="ZoneIdType">
    <xsd:restriction base="xsd:integer">
      <xsd:minInclusive value="1"/>
      <xsd:maxInclusive value="32"/>
    </xsd:restriction>
  </xsd:simpleType>

</xsd:schema>
```

GLOSSARY

A

answer

Network resources that respond to user queries. As with domains and source addresses, answers are configured at the primary GSSM by identifying a resource of a particular type on your GSS network to which queries can be directed and which can provide your user's D-proxy with the address of a valid host to serve their request. There are three types of possible Answers on an GSS network:

- **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 A balance method is an 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, typically a web browser or multimedia stream player, that makes Domain Name System (DNS) requests for domains managed by the GSS.

Cisco Network Registrar (CNR When coupled with GSS, it extends the product's capabilities and allows GSS to migrate to the top-level of the DNS hierarchy. This permits GSS to behave like a DNS appliance and simplifies the process of managing and configuring the DNS infrastructure.

content provider Customer deploying content on a Content Delivery Network (CDN), or purchasing 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 you specify, returning the online status of the device.

customer Cisco customer purchasing GSS hardware, software, or services. Typically, an Internet service provider (ISP), application service provider (ASP), or enterprise customer.

D

data center Collection of centrally located devices (content servers, transaction servers, or web caches).

Distributed Denial of Service (DDoS) A 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 A 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 The central configuration and routing concept of the GSS, allowing 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
The client's local name server, which makes iterative DNS queries on behalf of a client. A single recursive query from a client may result in many iterative queries from a D-proxy. Also referred to as local domain name server (LDNS).

DRP
Director Response Protocol (DRP). The GSS uses DRP to communicate with the probing devices, called DRP agents, in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems. You can use any Cisco router that is capable of supporting the DRP agent software and can measure ICMP echo-based RTT as the probing device in a zone. The GSS communicates with the IOS-based router using the DRP ICMP echo-based RTT query and response method.

F

fully qualified domain name (FQDN)
Domain name that specifies the named node's absolute location relative to the Domain Name System (DNS) root in the DNS hierarchy.

G

Global 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 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 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 Any 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 group for administrative and/or load balancing purposes.

HTTP HEAD Used when the GSS answer you are testing is a VIP associated with a 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 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 you are testing is a VIP associated with a SLB device such as a CSS or CSM, the ICMP keepalive type pings the configured VIP address (or a shared keepalive address). Online status is determined by a response from the targeted address, indicating simple connectivity to the network.

K

KAL-AP

Keepalive type used when the GSS answer you are testing is a VIP associated with a SLB device such as a CSS or CSM. The KAL-AP keepalive type sends a detailed query to both a primary (master) and secondary (backup) VIP address 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 Global Site Selector product uses both primary keepalive and secondary keepalive IP addresses.

See keepalive method.

keepalive method

Protocol or strategy used to determine whether a device is online, for example, ICMP, TCP, KAL-AP, HTTP HEAD, and CRA round-trip time.

L

LDNS

The Local Domain Name Server for a client.

load threshold

A 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 data center.

N

name server (NS) Publicly or privately addressable Domain Name System (DNS) server that resolves DNS names to IP addresses. Name servers are used by the GSS for name server forwarding, in which queries that the GSS cannot resolve are forwarded to a designated name server that can resolve them.

NS (keepalive) Keepalive that is used when the GSS answer you are testing is a Name Server, the Name Server keepalive type sends a query for a domain you specify to a name server at an address you provide. Online status is determined by the ability of the name server to resolve the domain to an address.

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 such 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 greatly expand the types of devices for which the GSS can perform load balancing, including remote caches, application servers, and more as well as SLBs.

O

order A 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 A 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 with 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, and a member will not be used unless all previous members fail to provide a suitable result. The Ordered List method is typically useful in managing resources at a single content site, for example, in a standalone deployment, or a redundant deployment in which the standby SLBs remain passive and are not used to serve requests.

origin server Machine that serves original or replicated content provider content.

owner Internal department or resource or external customer associated with a group of GSS resources such as domain lists, answer groups, and so on.

P

PDB

The proximity database (PDB) 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 residing in GSS memory (the answer with the lowest RTT time) and sends the answer to the requesting D-proxy. If the PDB proximity process is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from probing devices in every zone in the proximity network, and puts the results into the PDB in GSS memory. The GSS supports a maximum of 500,000 entries in the PDB.

probing

Probing refers to the process of measuring RTT from one probing device (DRP agent) to a requesting D-proxy device. Probe management is the intelligence behind each GSS device's interaction with the probing device in a zone. Within each zone, there must be at least one probing device and, optionally, a backup probing device. Upon failure of the primary probing device, the probes are redirected to the backup device. Once the primary probing device becomes available, probes are redirected back to the primary probing device. The GSS supports two type of probing methods: direct probing and refresh probing.

proximity

The GSS provides the ability to answer DNS requests with the most proximate answers relative to the requesting D-proxy. In this context, proximity refers to the distance or delay in terms of network topology, not geographical distance, between the requesting client's D-proxy and its answer. To determine the most proximate answer, the GSS communicates with a probing device, a Cisco IOS-based router, located in each proximity zone to gather round-trip time (RTT) metric information measured between the requesting client's D-proxy and the zone. Each GSS directs client requests to an available server with the lowest RTT value.

R

region

Grouping of GSS locations with common geographic attributes that is used to organize GSS resources.

round robin A 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. In this way, the GSS is able to resolve requests by evenly distributing the load amongst possible answers at both local- and remote content sites. 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 "active standby" site that serves requests.

RTT Round-trip time (RTT). The GSS transmits DRP queries to one or more probing devices in the GSS network, instructing the DRP agent in the probing device to probe specific D-proxy IP addresses. Each probing device responds to the query by using a standard protocol such as ICMP or TCP to measure the RTT between the DRP agent in the zone and the IP address of the requesting client's D-proxy device. From the RTT values in the PDB, the GSS selects the zone with the smallest RTT value as the most proximate zone containing the answer for the client's D-proxy request.

S

Scripted keepalive Keepalive type used when the GSS answer you are testing is a VIP associated with a SLB device such as a CSS or CSM. The Scripted Kal keepalive type is used to probe third-party devices and obtain the load information. Scripted keepalive uses the SNMP get request to fetch the load information from the target device.

Secure Socket Layer (SSL) Industry-standard method for protecting and encrypting web communication.

server load balancer (SLB) Network device that balances content requests to network resources based on content rules and real-time load and availability data collected from those devices. Server load balancers like the Cisco Content Services Switch (CSS), 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 providing 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 The 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 always 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 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 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 A client or set of clients receiving a certain style of DNS routing. Subscribers often pay for application services from the GSS customer.

T

TCP A TCP keepalive is used when the GSS answer that you are testing is to a GSLB devices may be something other than a CSS or CSM. These GSLB remote devices could 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 A series of specific client and server interactions that are logically connected to a single activity. For example, 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.

VIP Virtual IP addresses (VIPs) are 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 to be efficiently routed to the proper host without exposing that device's internal IP addresses to external users. When directed to a VIP by an 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) IOS feature for packet interception.

Web Network Services (WebNS) VxWorks-based operating system and software that runs on the Content Services Switch (CSS).

weight A balance method configuration option that is 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.

- 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 A balance method similar to round robin in which 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" factors is assigned to each answer, biasing the GSS toward certain servers such that they get picked more often.

Z

zone A customer network can be logically partioned into "zones" based on the arrangement of devices and network partioned 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 probing device that is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one probing device to a requesting D-proxy device.

INDEX