CHAPTER 9

Configuring Network Proximity

This chapter describes how to configure a GSS to perform network proximity to determine the best (most proximate) resource for handling global load-balancing requests.

This chapter contains the following major sections:

Each GSS supports a comprehensive set of **show** CLI commands to display network proximity statistics for the device. In addition, the primary GSSM GUI displays statistics about proximity operation for the GSS network. See Chapter 13, Displaying GSS Global Server Load-Balancing Statistics, for details about viewing network proximity statistics.

Network Proximity Overview

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

To determine the most proximate answer, the GSS communicates with proximity probing agents 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 probing agent can be either a Cisco IOS-based router or another GSS configured as a DRP agent.

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

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 a maximum of 32 zones. Within each zone, there is an active proximity probing agent that is configured to accept probing instructions from any GSS device. Probing refers to the process of measuring RTT from one proximity probing agent to a requesting D-proxy.

A location is a method to logically group devices in data centers for administrative purposes. A location can represent a physical point, such as a building or a rack. When you use the GSS to perform network proximity, each location must be assigned to a zone. In addition, you assign each answer used in a GSS proximity DNS rule to a location that is associated with a zone. This configuration hierarchy informs the GSS about resources when determining the most proximate answer.

Probe Management and Probing

Probe management is the intelligence behind each GSS device's interaction with the proximity probing agent in a zone. Within each zone, there must be at least one proximity probing agent and, optionally, a backup proximity probing agent. If the primary proximity probing agent fails, the probes are redirected to the backup device. Once the primary proximity probing agent becomes available, probes are redirected back to the primary proximity probing agent.

The GSS uses Director Response Protocol (DRP) to communicate with the proximity probing agents (called DRP agents) in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems.The GSS communicates with the proximity probing agent using the DRP RTT query and response method.

You can use another GSS as the proximity probing agent in a zone by enabling the DRP agent in the GSS. The GSS acting as a DRP agent supports ICMP, TCP, and path-probe RTT. You may also use any Cisco router as the proximity probing agent in a zone that can support the DRP agent software and measure ICMP or TCP; however, path-probe is not supported in the Cisco IOS router or other traditional DRP agent devices.

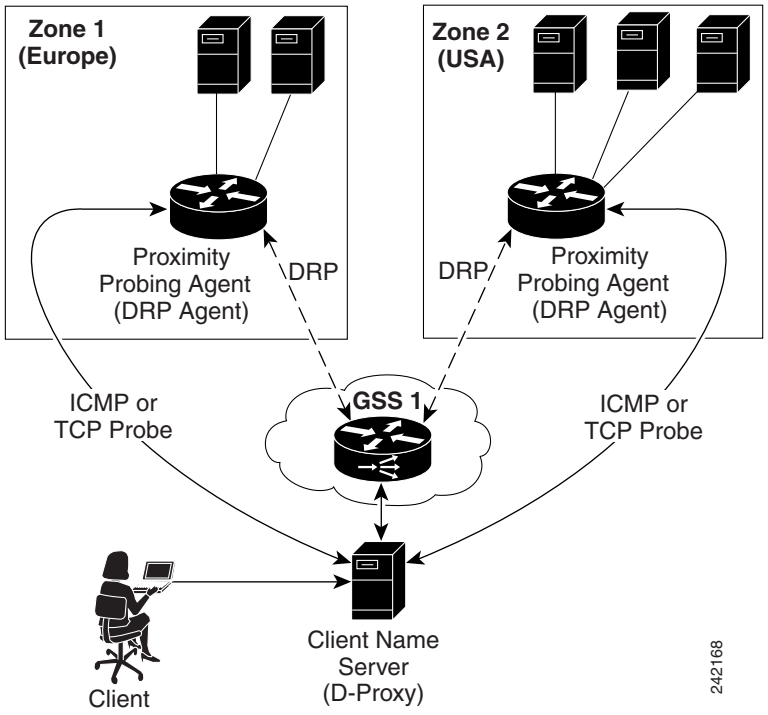
Each DRP agent accepts probing instructions from the GSS and returns probing results to the GSS based on the DRP protocol. DRP allows for the authentication of packets exchanged between the DRP agent and the GSS.

The GSS transmits DRP queries to one or more proximity probing agents in the GSS network, instructing the DRP agent in the proximity probing agent to probe specific D-proxy IP addresses. Each proximity probing agent responds to the query by using a standard protocol, such as ICMP or TCP, to measure the RTT between the DRP agent in the zone and the IP address of the requesting client's D-proxy device.

When the GSS receives a request from a D-proxy, it decides if it can provide a proximate answer. If the GSS is unable to determine a proximate answer from the proximity database (PDB), it sends a probe to one or more proximity probing agents to get proximity information between those proximity probing agents and the new D-proxy. After the GSS receives the probing results, it adds the RTT information to the PDB.

Figure 9-1 shows the probing process between a GSS (DRP client) and a proximity probing agent (DRP agent).

Figure 9-1 DRP Communication in a GSS Network



The GSS supports two types of probing methods:

- Direct Probing—Direct probing occurs between the GSS and DRP agents when the GSS creates a dynamic entry in the PDB as the result of receiving a new D-proxy IP address. Direct probing also occurs when you specify alternative IP addresses as targets for the proximity probing agents to obtain RTT data and add static entries in the PDB. The GSS initiates direct probing to the DRP agent when a request is made for a new D-proxy IP address entry. Through direct probing, the GSS automatically sends probe requests to the DRP agent in each zone to obtain initial probe information as quickly and efficiently as possible for the new entries in the PDB.
- Refresh Probing—The GSS periodically reprobes the actively used D-proxies to obtain the most up-to-date RTT values and store these values in the PDB. The RTT values reflect recent network changes. The refresh probe interval is a user-configured selection.

Note Static entries in the PDB created with static RTT values do not use direct or refresh probing. The configured static RTT is always returned during proximity lookup regardless of the configured acceptable available percentage of zones.

Proximity Database

The PDB provides the core intelligence for all proximity-based decisions made by a GSS. Proximity lookup occurs when a DNS rule is matched and the associated clause has the proximity option enabled. When the GSS receives a request from a D-proxy and decides that a proximity response should be provided, the GSS identifies the most proximate answer (the answer with the smallest RTT time) from the PDB that resides in GSS memory and sends that answer to the requesting D-proxy. If the PDB is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from proximity probing agents in every zone in the proximity network, and puts the results in the PDB.

For example, a GSS communicates with three zones to determine the most proximate answer and receives the following RTT values from the proximity probing agents in each zone to a particular client D-proxy:

- Zone1 = 100 ms
- Zone2 = 120 ms
- Zone3 = 150 ms

From the three RTT values in the PDB, the GSS selects Zone1 as the most proximate zone for the client's D-proxy request because it has the smallest RTT value.

The GSS supports a maximum of 500,000 D-proxy IP address entries in the PDB table, including both dynamic and static entries. The GSS creates dynamic entries in the PDB as the result of requests for new D-proxy IP addresses. If necessary, you can add static entries to the PDB by specifying permanent RTT values (gathered by other means), and optionally, alternative IP addresses to probe.

The primary GSSM supports the creation of proximity groups that allow you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its PDB as a single entry. Instead of multiple PDB entries, the GSS uses only one entry in the PDB for multiple D-proxies. The GSS treats all D-proxies in a proximity group as a single D-proxy when responding to DNS requests with the most proximate answers. Requests from D-proxies within the same proximity group receive the RTT values from the database entry for the group. The benefits of proximity grouping are as follows:

- Fewer probing activities performed by the GSS
- Less space required for the PDB
- Greater user flexibility in assigning alternative probing targets or static proximity metrics to a group

The dynamic entries in the PDB age out based on the user-specified global inactivity setting to keep the PDB size manageable. The inactivity timeout setting defines the maximum period of time that can occur without a PDB entry receiving a lookup request, after which the GSS deletes the entry from the PDB.

When the total number of entries in the PDB exceeds 480,000, the GSS automatically removes the least recently used entries. The GSS determines the least recently used entries as those dynamic entries in the PDB that have not been hit within a fixed cutoff time of 60 minutes (one hour). The GSS does not automatically remove static entries from the PDB. You must manually delete PDB static entries from the GSS CLI.

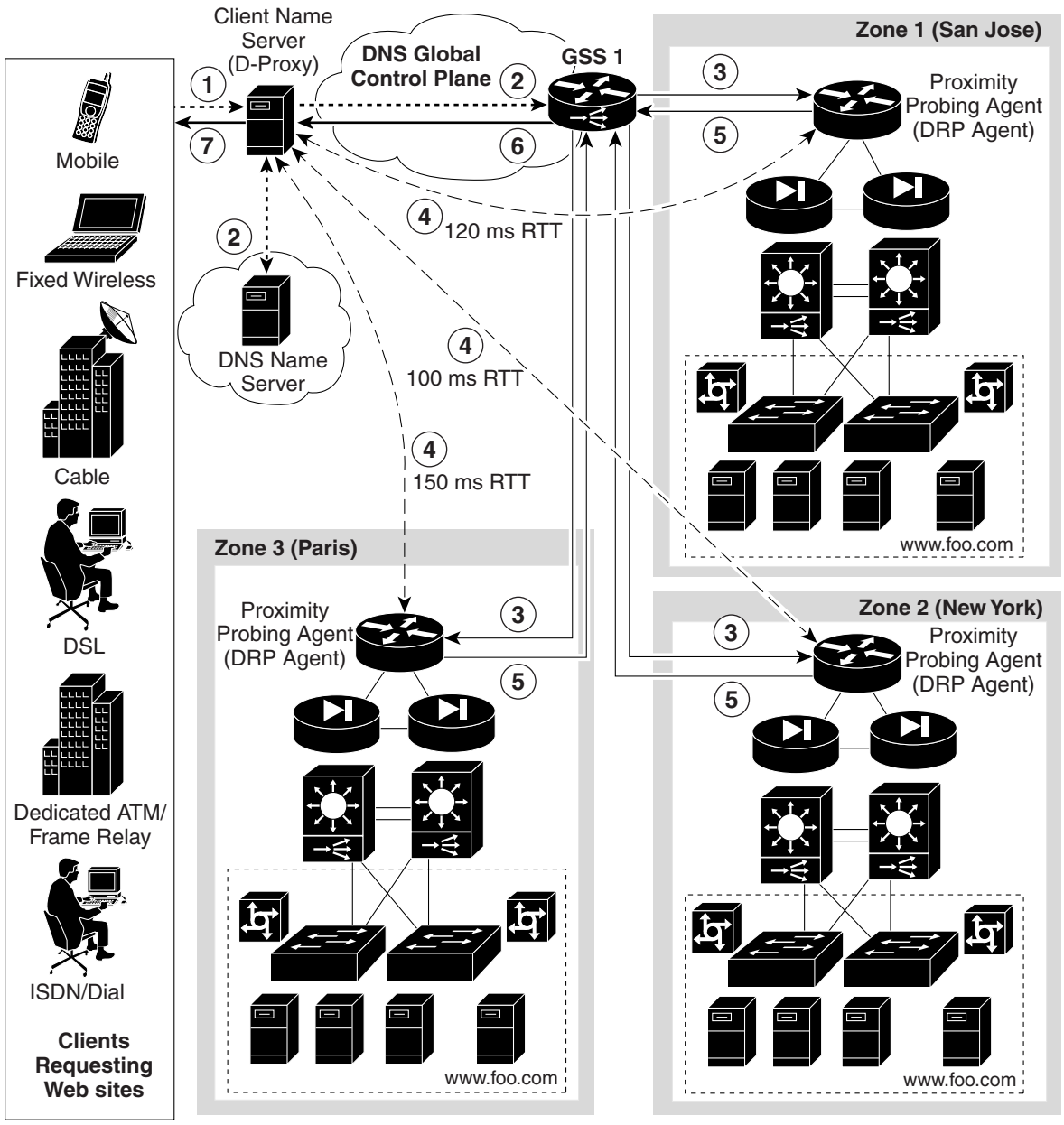
When the PDB reaches a maximum of 500,000 entries, the GSS does not add entries to the PDB and any new requests for answers result in a failure. The GSS tracks how many entries are dropped when the maximum limit has been reached. Once the number of PDB entries drops below 500,000, the GSS resumes adding new entries to the PDB.

Example of Network Proximity

The process outlined below describes how the GSS interacts with the proximity probing agents in multiple zones to perform network proximity. See Figure 9-2 for an illustration of the following steps.

1. A client performs an HTTP request for www.foo.com. The content for this website is supported at three different data centers.
2. The DNS global control plane infrastructure processes this request and directs the client D-proxy to GSS 1. The GSS offloads the site selection process from the DNS global control plane. The client's local D-proxy queries GSS1 for the IP address associated with www.foo.com. The GSS accepts the DNS query.
3. If the request matches a proximity DNS rule configured on the GSS, the GSS performs an internal PDB lookup. If the lookup fails, the GSS sends DRP queries to the DRP agent configured for each zone.
4. When the DRP agent in each zone receives a DRP request, it measures the RTT from the associated zone back to the requesting client D-proxy device, using either ICMP, TCP, or a path-probe.
5. After calculating DRP RTT metrics, the DRP agents send their replies to the GSS. The GSS sorts the DRP RTT replies from the DRP agents to identify the best (smallest) RTT metric. The DRP agent then returns the smallest RTT metric that identifies the closest zone, which in Figure 9-2 is Zone 2 (New York).
6. The GSS returns to the client's local D-proxy one or more IP address records (DNS A resource records) that match the DNS rule and correspond to the best or most proximate server (www.foo.com) located in Zone 2 (New York).
7. The client's local D-proxy returns the IP address that corresponds to www.foo.com to the client that originated the request. The client transparently connects to the server in Zone 2 for www.foo.com.

Figure 9-2 Network Proximity Using the Cisco Global Site Selector



Proximity Network Design Guidelines

When developing your proximity network, ensure that you include a sufficient number of GSS devices to support the expected load. Follow these guidelines when designing your proximity network:

- Decide how many zones you require for your proximity network based on your current network configuration and the level of proximity that you require for your network. A maximum of 32 zones is allowed within each GSS proximity environment. You can change the zone configuration at any time by deleting or adding a zone, or by moving a zone from one location to another location.

- For each zone, identify the proximity probing agent and optionally the back up for the proximity probing agent. Each proximity probing agent represents the topological location of its associated zone and also reflects the zone's expected network behavior in terms of connectivity to the Internet. The proximity probing agent is the DRP agent located within the zone.
- Each GSS network can contain a maximum of 16 GSS devices. You can add or delete GSS devices at any time. The GSS does not have to reside within a zone.
- To use proximity, you must do the following:
  - Associate a proximity zone with a location.
  - Assign a location that is associated with a proximity zone to an answer.

  To use an answer group with a proximity balance method, the answers in the answer group must be contained in locations that are tied to a zone.

Network Proximity Quick Start Guide

Table 9-1 provides a quick overview of the steps required to configure the GSS for proximity network operation. Each step includes the primary GSSM CLI command required to complete the task. For detailed procedures to configure the GSS for proximity, see the sections that follow the table.

Table 9-1 Proximity Configuration Quick Start

Task and Command Example

1. Log in to the CLI of each GSS in the network, enable privileged EXEC mode, and synchronize its system clock with an NTP server.
For example, enter:
`gssm1.example.com> enable`
`gssm1.example.com# config`
`gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3`
`gssm1.example.com(config)# ntp enable`

2. Configure a Cisco router or GSS as a DRP agent in one or more proximity zones.

3. Enter the global server load-balancing configuration mode.
For example, enter:
`gssm1.example.com(config)# gslb`
`gssm1.example.com(config-gslb)#`

4. Configure a proximity zone from the primary GSSM by entering the **zone** command. For example, enter: `gssm1.example.com(config-gslb)# zone Z1 index 1 probe 192.168.11.1 backup probe 192.168.11.5`

5. Access the proximity properties configuration mode by entering the **proximity-properties** command in global server load-balancing configuration mode.
For example, enter:
`gssm1.example.com(config-gslb)# proximity-properties`
`gssm1.example.com(config-gslb-proxprop)#`

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

6. From the proximity properties configuration mode, enable proximity.
 	
For example, enter:
 	
`gssm1.example.com(config-gslb-proxprop)# enable`
`gssm1.example.com(config-gslb-proxprop)# exit`
`gssm1.example.com(config-gslb)#`

7. Configure global proximity configuration default settings using the following commands in proximity properties configuration mode: • **mask** *netmask*—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of supported D-proxies in the PDB. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). • **timeout** *minutes*—Specifies the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry. • **equivalence** *number*—Specifies a percentage value that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Use this command to adjust the granularity of the proximity decision process. • **refresh-interval** *hours*—Specifies the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. • **discovery-sequence**—Specifies the type of probe method (TCP or ICMP) that the Cisco IOS-based router uses initially during the probe discovery process with the requesting client's D-proxy. If the router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically uses the other probe method to contact the D-proxy. • **fallback-probe-method path-probe**—Enables the path-probe method as the fallback method that the GSS (acting as a DRP agent) uses when both the TCP and ICMP probe methods fail. **Note** The GSS supports the path-probe method only when you have it configured as a DRP agent (see the "Configuring the GSS as a DRP Agent" section). By default, the path-probe method is not enabled. • **acceptable-rtt** *number*—Specifies a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. Use this command to adjust the granularity of the proximity decision process. • **acceptable-zone** *number*—Specifies a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The value specifies the percentage of all zones configured and used for a DNS rule and answer group.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

• **wait enable**—Enables the GSS proximity wait-state.
• **authentication drp enable—**Enables the DRP authentication state.
• **key drp—**If you enabled **authentication drp enable** and no DRP keys exist for the GSS, use this command to create a DRP authentication key. Repeat the command to make additional keys. Each DRP key includes a key identification number and a key authentication string.
See the "Configuring Proximity" section for a complete description of these settings.
For example, to enable global proximity and specify settings, enter:
`gssm1.example.com(config-gslb)# proximity-properties`
`gssm1.example.com(config-gslb-proxprop)# enable`
`gssm1.example.com(config-gslb-proxprop)# mask 255.255.255.255`
`gssm1.example.com(config-gslb-proxprop)# timeout 4320`
`gssm1.example.com(config-gslb-proxprop)# equivalence 20`
`gssm1.example.com(config-gslb-proxprop)# refresh-interval 6`
`gssm1.example.com(config-gslb-proxprop)# discovery-sequence icmp`
`gssm1.example.com(config-gslb-proxprop)# acceptable-rtt 100`
`gssm1.example.com(config-gslb-proxprop)# acceptable-zone 40`
`gssm1.example.com(config-gslb-proxprop)# exit`
`gssm1.example.com(config-gslb)#`

8. (Optional) Enable DRP authentication and create a DRP key by entering the **authentication drp enable** and **key drp** commands.
For example, to create two new DRP keys, enter:
`gssm1.example.com(config-gslb)# proximity-properties`
`gssm1.example.com(config-gslb-proxprop)# enable`
`gssm1.example.com(config-gslb-proxprop)# key drp 10 DRPKEY1`
`gssm1.example.com(config-gslb-proxprop)# key drp 20 DRPKEY2`
`gssm1.example.com(config-gslb-proxprop)# exit`
`gssm1.example.com(config-gslb)#`

9. (Optional) Associate a location to a proximity zone by using the **location** command in global server load-balancing configuration mode. Repeat this step for each location that you want to assign to a proximity zone.
For example, to associate the zone z3 with the location London, enter:
`gssm1.example.com(config-gslb)# location London zone z3`
`gssm1.example.com(config-gslb)#`

10. (Optional) Assign a location associated with a proximity zone to an answer by using the **answer vip** *ip_address* command in global server load-balancing configuration mode. Repeat this step for each answer that you want to assign to an associated proximity location.
For example, to associate the location "Paris" with the VIP answer called "SEC-PARIS2" enter:
`gssm1.example.com(config-gslb)# answer vip 172.16.27.6 name SEC-PARIS2 location Paris`
`gssm1.example.com(config-ansvip[ans-ip])`

11. Develop your DNS rule by using the **dns rule** command.
For example, enter:
`gssm1.example.com(config)# gslb`
`gssm1.example.com(config-gslb)# dns rule drule03 owner WEB-SERVICES source-address-list WEB-GLOBAL-LISTS domain-list E-COMMERCE query A`
`gssm1.example.com(config-gslb-rule[rule-name])#`

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

12. Configure Balance Clause 1 for the DNS rule bv using the **clause** command and the **proximity enable** option to enable proximity for the DNS rule.
 	
For example, enter:
 	
`gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group method ordered ANSGRP-VIP-03 proximity enable`
`gssm1.example.com(config-gslb-rule[rule-name])#`

13. (Optional) Modify other **clause** command settings for proximity as appropriate. See the "Adding Proximity to a DNS Rule that uses VIP-Type Answer Groups" section for a complete description of all settings available for the **clause** command. You can modify the following proximity settings: • **rtt** *number*—Changes the proximity-acceptable RTT for the balance clause to a different value from the global proximity configuration. • **wait enable/disable** —Changes the proximity wait state to a different setting than the global proximity configuration. • **zone** *number*—Changes the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration. For example, to set up Balance Clause 1 with proximity for a previously created DNS rule, enter: `gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group ANSGRP-VIP-03 method ordered proximity enable rtt 75 zone 50`

14. Using the **clause** command again, repeat Steps 12 and 13 for Balance Clause 2.
 	
For example, enter:
 	
`gssm1.example.com(config-gslb-rule[rule-name])# clause 2 vip-group ANSGRP-VIP-03 method ordered proximity enable rtt 120 zone 55`
`gssm1.example.com(config-gslb-rule[rule-name])#`

15. Reenter the **clause** command for Balance Clause 3, and then repeat Steps 12 and 13.

16. (Optional) Group multiple D-proxy IP addresses as a single entry in the PDB to reduce probing and to take up less space, access the global server load-balancing configuration mode, and create a proximity group at the primary GSSM. Do so by using the **proximity group** command to add multiple D-proxy IP addresses and subnet masks to the group.
 	
For example, enter:
 	
`gssm1.example.com# config`
`gssm1.example.com(config)# gslb`
`gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip 192.168.3.0 netmask 255.255.255.0`

17. (Optional) Add static proximity entries to the PDB of a GSS device in your network, access the global server load-balancing configuration mode, and use the **proximity assign** command to create static entries.
 	
For example, enter:
 	
`gssm1.example.com# config`
`gssm1.example.com(config)# gslb`
`gssm1.example.com(config-gslb)# proximity assign group ISP2 zone-data "1:100,2:200,3:300,4:400,5:500"`

Configuring the GSS as a DRP Agent

The DRP agent module allows you to configure a GSS to act as a DRP agent, either as dedicated DRP agent device or in combination with its global server load-balancing functionality.

This section explains the features of the GSS DRP agent and contains the following topics:

The GSS DRP agent supports three types of RTT probing mechanisms: ICMP, TCP, and path-probe. Path-probe is not supported in traditional DRP agent devices, such as the Cisco IOS router.

The ICMP and TCP probing mechanisms on the GSS DRP agent are identical to those on the Cisco IOS router. To obtain configuration commands for ICMP and TCP probes, see the following website:

http://cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/gss4400series/v2.0/command/reference/DRPagent.html#wp1619127

Path-probe is a mechanism introduced in version 2.0, which calculates the RTT when the querying D-proxy is behind a firewall. When the D-proxy is behind a firewall, the GSS DRP agent is unable to reach it using the conventional ICMP and TCP probing mechanisms. After trying the conventional probing mechanisms, the GSS DRP agent uses path-probe as the fallback mechanism to calculate the RTT of the D-proxy. In the path-probe process, all participating DRP agents use traceroute to trace their paths to the D-proxy and report their paths (along with the RTTS) to the GSS.

To obtain configuration commands for path-probe, see the following website:

http://cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/gss4400series/v2.0/command/reference/DRPagent.html#wp1733714

GSS DRP Agent Configuration Quick Start

Table 9-2 provides a quick overview of the steps required to configure the GSS as a DRP agent. Each step includes the primary GSSM CLI command required to complete the task. For the procedures to configure the GSS as a DRP agent, see the sections that follow the table.

Table 9-2 GSS DRP Agent Configuration Quick Start

Task and Command Example

1. Log on to the GSS, enable the privileged EXEC mode, and enter the configuration mode.
For example, enter:
`gssm1.example.com> enable`
`gssm1.example.com# config`

2. Enter the DRP agent configuration mode and enable the DRP agent.
For example, enter:
`gssm1.example.com(config)# drp`
`gssm1.example.com(config-drp)# enable`

Table 9-2 GSS DRP Agent Configuration Quick Start (continued)

Task and Command Example
3. Enable the DRP authentication key chain ID. For example, enter: `gssm1.example.com(config-drp)# authentication key 240`

4. Enter the path probe configuration mode and configure the parameters of the path probe.
For example, enter:
`gssm1.example.com(config-drp)# probe path-rtt`
`gssm1.example.com(config-drp-path-rtt)# probe-type udp`
`gssm1.example.com(config-drp-path-rtt)# burst-size 15`
`gssm1.example.com(config-drp-path-rtt)# timeout 3`
`gssm1.example.com(config-drp-path-rtt)# destination-port 555`
`gssm1.example.com(config-drp-path-rtt)# sourceport static 65530`
`gssm1.example.com(config-drp-path-rtt)# init-ttl 20`
`gssm1.example.com(config-drp-path-rtt)# max-failure-ttl 12`
`gssm1.example.com(config-drp-path-rtt)# max-ttl`
`gssm1.example.com(config-drp-path-rtt)# exit`
`gssm1.example.com(config-drp)#`

5. Enter the TCP probe configuration mode and configure the TCP probe parameters.
For example, enter:
`gssm1.example.com(config-drp)# probe tcp-rtt`
`gssm1.example.com(config-drp-tcp-rttprobe)# destination-port 17`
`gssm1.example.com(config-drp-tcp-rttprobe)# sourceport dynamic`
`gssm1.example.com(config-drp-tcp-rttprobe)# timeout 4`
`gssm1.example.com(config-drp-tcp-rttprobe)# exit`
`gssm1.example.com(config-drp)#`

6. Enter the ICMP probe configuration mode and configure the timeout value for the ICMP probe.
For example, enter:
`gssm1.example.com(config-drp)# probe icmp-rtt timeout 5`
`gssm1.example.com(config-drp-icmp-rtt)# exit`
`gssm1.example.com(config-drp)# exit`
`gssm1.example.com(config)# exit`

Enabling the GSS DRP Agent

You can enable the DRP agent on the GSS by using the **enable** command in DRP agent configuration mode.

The syntax of this command is as follows:

enable

To disable the DRP agent, use the **no** form of the command.

To enable the DRP agent, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# enable
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To disable the DRP agent, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# no enable
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Enabling the DRP Authentication Key Chain ID

You can enable a DRP authentication key chain ID by using the **authentication key** command in DRP agent configuration mode.

The syntax of this command is as follows:

authentication key *key-id*

The *key-id* argument is the DRP keychain identifier. Enter a value from 0 to 255. To disable a keychain identifier, use the **no** form of the command.

To enable the DRP keychain ID 240, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# authentication key 240
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To disable the keychain ID 240, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# no authentication key 240
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the ICMP Probe Timeout Parameter

You can configure the ICMP probe timeout parameter by using the **probe icmp-rtt timeout** command in DRP agent configuration mode.

The syntax of this command is as follows:

probe icmp-rtt timeout *time*

The *time* argument is the timeout value in seconds. Enter a value from 1 to 5. The default is 3. To configure the probe not to time out, use the **no timeout** command.

To configure the ICMP probe timeout to 5 seconds, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe icmp-rtt timeout 5
gssm1.example.com(config-drp-icmp-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the ICMP probe not to time out, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe icmp-rtt
gssm1.example.com(config-drp-icmp-rtt)# no timeout
gssm1.example.com(config-drp-icmp-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Path Probe Parameters

You can enter path probe configuration mode to configure the path probe parameters by using the **probe path-rtt** command in DRP configuration mode.

The syntax of this command is as follows:

probe path-rtt

To enter path probe configuration mode, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)#
```

This section contains the following topics:

Configuring the Packet Type

You can specify the type of packet to use for path probing by using the **probe-type** command in path probe configuration mode.

The syntax of this command is as follows:

probe-type {**tcp** | **udp**}

The keywords for this command are as follows:

- **tcp**—TCP packet.
- **udp**—UPD packet.

The default is a TCP-SYN-ACK packet.

To set the path probe packet type to UDP, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# probe-type udp
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Burst Size

You can configure the number of TCP-SYN-ACK packets to send at a time by using the **burst-size** command in path probe configuration mode.

The syntax of this command is as follows:

burst-size *burst_size*

The *burst-size* argument is the number of packets to send at a time. Enter a value of 1 to 20. The default is 5. To specify that burst sizes are not sent, use the **no** form of the command.

To set the burst size to 15 packets, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# burst-size 15
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no burst size, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no burst-size
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Timeout

You can configure the timeout value of the path probe by using the **timeout** command in path probe configuration mode.

The syntax of this command is as follows:

timeout *time*

The *time* argument is the number of seconds to elapse before the probe times out. Enter a value of 1 to 10. The default is 3. To configure the probe not to time out, use the **no timeout** command.

To set the timeout value to 3 seconds, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# timeout 3
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe not to time out, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no timeout
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Destination Port

You can configure the destination port of the path probe by using the **destination-port** command in path probe configuration mode.

The syntax of this command is as follows:

destination-port *port*

The *port* argument is the destination port number. Enter a value of 1 to 65535. The default is 53. To configure the probe with no destination port number, use the **no destination-port** command.

To set the destination port to 555, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# destination-port 555
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-dr
```

To configure the probe with no destination port number, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no destination-port
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Source Port

You can configure the source port of the path probe by using the **sourceport** command in path probe configuration mode.

The syntax of this command is as follows:

sourceport {**dynamic** | **static**} *port*

The keywords and arguments are as follows:

- **dynamic**—Specifies a dynamic path probe source port.
- **static**—Specifies a static path probe source port.
- *port*—Port number. Enter a value from 1 to 65535. The default is 53.

To configure the probe with no source port number, use the **no** form of the command.

To set the static source port to 65530, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# sourceport static 65530
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no static source port number, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no sourceport static
gssm1.example.com(config-drp-path-rtt)# exit
```

```
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring an Initial Time-to-Live

You can configure an initial Time-to-Live for the path probe by using the **init-ttl** command in path probe configuration mode.

The syntax of this command is as follows:

init-ttl *time*

The *time* argument is the initial Time-to-Live in seconds. Enter a value from 1 to 32. The default is 1. To configure the probe with no initial Time-to-Live, use the **no init-ttl** command.

To set the initial Time-to-Live to 20 seconds, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# init-ttl 20
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no initial Time-to-Live, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no init-ttl
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Number of Last Successive Failure Packets

You can configure an acceptable number of last successive failure packets the path probe by using the **max-failure-ttl** command in path probe configuration mode.

The syntax of this command is as follows:

max-failure-ttl *number_packets*

The *number_packets* argument is the acceptable number of last successive failure packets. Enter a value from 1 to 32. The default is 5. To configure the probe with no acceptable number of last successive failure packets, use the **no max-failure-ttl** command.

To set the acceptable number of last successive failure packets to 12, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# max-failure-ttl 12
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no acceptable number of last successive failure packets, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no max-failure-ttl
```

```
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Maximum Time-to-Live

You can configure the maximum Time-to-Live for path probing by using the **max-ttl** command in path probe configuration mode.

The syntax of this command is as follows:

max-ttl *number_packets*

The *number_packets* argument is the maximum Time-to-Live value in seconds. Enter a value from 1 to 255. The default is 32. To configure the probe with no maximum Time-to-Live, use the **no max-ttl** command.

To set the maximum Time-to-Live to 37, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# max-ttl 37
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no maximum Time-to-Live, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe path-rtt
gssm1.example.com(config-drp-path-rtt)# no max-ttl
gssm1.example.com(config-drp-path-rtt)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the TCP Probe Parameters

You can enter TCP RTT configuration mode to configure the TCP probe parameters by using the **probe tcp-rtt** command in DRP configuration mode.

The syntax of this command is as follows:

probe tcp-rtt

To enter TCP RTT Probe configuration mode, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)#
```

This section contains the following topics:

Configuring the Destination Port

You can configure the destination port of the TCP probe by using the **destination-port** command in TCP probe configuration mode.

The syntax of this command is as follows:

destination-port *port*

The *port* argument is the destination port number. Enter a value of 1 to 65535. The default is 53. To configure the probe with no destination port number, use the **no destination-port** command.

To set the probe destination port to 555, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)# destination-port 555
gssm1.example.com(config-drp-tcp-rttprobe)# exit
gssm1.example.com(config-drp)
```

To configure the probe with no destination port number, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttport)# no destination-port
gssm1.example.com(config-drp-tcp-rttport)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Source Port

You can configure the source port of the TCP probe by using the **sourceport** command in TCP probe configuration mode.

The syntax of this command is as follows:

sourceport {**dynamic** | **static**} *port*

The keywords and arguments are as follows:

- **dynamic**—Specifies a dynamic path probe source port.
- **static**—Specifies a static path probe source port.
- *port*—Port number. Enter a value from 1 to 65535. The default is 53.

To configure the TCP probe with no source port number, use the **no** form of the command.

To set the probe static source port to 65530, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)# sourceport static 65530
gssm1.example.com(config-drp-tcp-rttprobe)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe with no static source port number, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)# no sourceport static
gssm1.example.com(config-drp-tcp-rttprobe)# exit
```

```
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring the Timeout

You can configure the timeout value of the TCP probe by using the **timeout** command in TCP probe configuration mode.

The syntax of this command is as follows:

timeout *timeout*

The *timeout* argument is the number of seconds to elapse before the probe times out. Enter a value of 1 to 10. The default is 3. To configure the probe so that it does not timeout, use the **no timeout** command.

To set the probe timeout value to 3 seconds, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)# timeout 3
gssm1.example.com(config-drp-tcp-rttprobe)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

To configure the probe so that it does not time out, enter:

```
gssm1.example.com(config)# drp
gssm1.example.com(config-drp)# probe tcp-rtt
gssm1.example.com(config-drp-tcp-rttprobe)# no timeout
gssm1.example.com(config-drp-tcp-rttprobe)# exit
gssm1.example.com(config-drp)# exit
gssm1.example.com(config)#
```

Configuring a Cisco Router as a DRP Agent

When you enable DRP on a Cisco router, the router gains the additional functionality of operating as a DRP agent in the GSS network. A DRP agent can communicate with multiple GSSs and support multiple distributed servers.

This section includes the following background information about choosing and configuring the Cisco router in each proximity zone as a DRP agent. It contains the following topics:

- Choosing a Cisco Router as a DRP Agent
- Configuring the DRP Agent
- Cisco IOS Release 12.1 Interoperability Considerations

Choosing a Cisco Router as a DRP Agent

When selecting a Cisco router as the DRP agent in a zone, you should ensure the following:

- The DRP agent is topologically close to each distributed server that it supports in the zone.
- The DRP agent in the Cisco IOS-based router is configured to perform ICMP or TCP echo-based RTT probing.

Configuring the DRP Agent

You can configure and maintain the DRP agent in the Cisco IOS-based router by performing the tasks described in the "Configuring a DRP Server Agent" section, of the *Cisco IOS IP Configuration Guide*. The Cisco IOS-based router must support the DRP protocol in a proximity zone. DRP is supported in the following Cisco IOS Release trains: 12.1, 12.1E, 12.2T, 12.2, 12.3, and later releases. ICMP probing is supported only in Cisco IOS Release 12.2T, 12.3, and later.

The GSS operates with Cisco IOS-based routers using the following DRP RTT probing methods: TCP ("DRP Server Agent") and ICMP ("ICMP ECHO-based RTT probing by DRP agents"). The Cisco IOS feature names shown in the Cisco Feature Navigator II are as follows: "DRP Server Agent" and "ICMP ECHO-based RTT probing by DRP agents."

The following process is required to configure a Cisco IOS-based router as a DRP agent:

1. Enable the DRP agent in the Cisco router.
2. Enable security for DRP by defining a standard access list that permits requests from only the GSS device. As a security measure, limit the source of valid DRP queries. If a standard IP access list is applied to the interface, the DRP agent responds only to DRP queries that originate from an IP address in the list. If no access list is configured, the DRP agent answers all queries.
3. Ensure that the router accepts DRP queries from the IP addresses associated with only the standard access list.
4. If necessary, set up Message Digest (MD5) authentication with passwords as another security measure. Enable the DRP authentication key chain, define the key chain, identify the keys associated with the key chain, and specify how long each key is to be valid. If MD5 authentication is configured on a DRP agent, the GSS device must be similarly configured to recognize messages from that MD5 authentication-configured DRP agent and any other DRP agents configured for MD5 authentication.

Cisco IOS Release 12.1 Interoperability Considerations

If you use a GSS in a network proximity zone configuration with a router running Cisco IOS Release 12.1, you should ensure the DRP authentication configuration is identical on both devices. For example, if you intend to perform DRP authentication between a GSS and a router running Release 12.1, ensure that you properly enable and configure authentication on both devices. The same is true if you choose not to use DRP authentication; you must disable authentication on both devices.

If you disable DRP authentication on a router running Cisco IOS Release 12.1 but enable DRP authentication on a GSS, all measurement probes sent by a GSS to the router will fail. This occurs because the router fails to recognize the DRP echo query packets sent by a GSS and the GSS cannot detect a potential failure of measurement packets sent to the router. The GSS identifies the router as being ONLINE in its **show statistics proximity probes detailed** CLI command, yet the measurement response packets monitored in the Measure Rx field do not increment. These two conditions may indicate a DRP authentication mismatch.

If the DRP probe requests fail between the GSS and a Cisco router running Release 12.1, even if the GSS indicates that the router is ONLINE, verify the DRP authentication configurations on both the GSS and the Cisco router as follows:

- For the Cisco router running IOS Release 12.1, enter the **show ip drp** command. If the line "`Authentication is enabled, using "test" key-chain`" appears in the output (where "test" is the name of your key-chain), DRP authentication is configured on the router. If this line does not appear in the output, DRP authentication is not configured.

- For the Primary GSSM, enter the **show gslb-config proximity-properties** command to view the state of the authentication drp enable setting (see the "Configuring Proximity" section for details).

Modify the DRP authentication configuration on either the router running Cisco IOS Release 12.1 or the primary GSSM and make them consistent to avoid a DRP authentication mismatch.

Logging in to the CLI and Enabling Privileged EXEC Mode

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

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

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

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

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

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

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

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

   If you are accessing the GSS remotely using Telnet or SSH, the CLI prompts you for the enable password. The default password is default. For more information about the enable password and configuring a new password, see the *Cisco Global Site Selector Getting Started Guide*.

   The prompt changes from the user-level EXEC right angle bracket (>) prompt to the privileged-level EXEC pound sign (#).

Synchronizing the GSS System Clock with an NTP Server

We strongly recommend that you synchronize the system clock of each GSS device in your network with a Network Time Protocol (NTP) server. NTP is a protocol designed to synchronize the clocks of computers over a network with a dedicated time server.

Synchronizing the system clock of each GSS ensures that the PDB and probing mechanisms function properly by having the GSS internal system clock remain constant and accurate within the network. Changes in the GSS system clock can affect the time stamp used by PDB entries and the probing mechanism used in a GSS.

You must specify the NTP server(s) for each GSS device operating in the proximity network before you enable proximity for those devices from the primary GSSM. This sequence ensures that the clocks of each GSS device are synchronized.

Note For details on logging in to a GSS device and enabling privileged EXEC mode at the CLI, see the "Creating Proximity Groups" section.

You can specify one or more NTP servers for GSS clock synchronization by using the **ntp-server** global configuration mode command.

The syntax of this CLI command is as follows:

ntp-server *ip_or_host*

The *ip_or_host* argument specifies the IP address or hostname of the NTP time server in your network that provides the clock synchronization. You can specify a maximum of four IP addresses or hostnames. Enter the IP address in dotted-decimal notation (for example, 172.16.1.2) or a mnemonic hostname (for example, myhost.mydomain.com).

You can enable the NTP service by using the **ntp enable** global configuration mode command.

The syntax of this command is as follows:

ntp enable

To specify the IP addresses of two NTP time servers for a GSS device and enable the NTP service, enter:

```
gssm1.example.com> enable
gssm1.example.com# config
gssm1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
gssm1.example.com(config)# ntp enable
```

Creating Zones Using the Primary GSSM CLI

A proximity zone is a logical grouping of network devices that also contains one active proximity probing agent and a possible backup proximity probing agent. A zone can be geographically related to a continent, a country, or a major city. Each zone can include one or more locations. A location is a method to logically group collocated devices for administrative purposes.

During the proximity selection process, the GSS chooses the most proximate zones that contain one or more valid answers based on RTT data received from the proximity probing agents configured in the zone. You can configure a proximity network with a maximum of 32 zones.

This section includes the following topics:

- Configuring a Proximity Zone
- Deleting a Proximity Zone
- Associating a Proximity Zone With a Location
- Associating a Proximity-Based Location with an Answer

Configuring a Proximity Zone

You can configure a proximity zone from the primary GSSM by using the **zone** command in global server load-balancing configuration mode.

The syntax of this command is as follows:

zone *name* {**index** *number* | **probe** *ip_address*} [**backup probe** *ip_address*]

The keywords and arguments are as follows:

- *name*—Zone name. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **index** *number*—Specifies the numerical identifier of the proximity zone. Enter an integer from 1 to 32. There is no default.
- **probe** *ip_address*— Specifies the IP address of the primary probe device that services this zone. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- **backup probe** *ip_address*—(Optional) Specifies the IP address of a backup probe device that services this zone. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

For example, enter:

```
gssm1.example.com(config-gslb)# zone Z1 index 1 probe 192.168.11.1 backup 192.168.11.5
```

To modify the properties for a previously created zone, enter:

```
gssm1.example.com(config-gslb)# zone Z1 index 1 probe 192.168.11.2 backup 192.168.11.9
```

Note You cannot modify the **index** value. To change the zone index, delete the zone (see the “Deleting a Proximity Zone” section), and then create a new zone containing a different index.

Deleting a Proximity Zone

Use the **no** form of the **zone** command to delete a zone.

For example, to delete zone “z1,” enter:

```
gssm1.example.com(config-gslb)# no zone Z1 index 1 probe 192.168.11.1 backup 192.168.11.5
```

or

```
gssm1.example.com(config-gslb)# no zone Z1
```

Associating a Proximity Zone With a Location

You can associate an existing proximity zone with a location by using the **location** command in global server load-balancing configuration mode. You can make the association for a new location or for an existing location. To display a list of existing locations, use the **show gslb-config location** command (see the “Displaying Resource Information” section in Chapter 2, Configuring Network Proximity, for more information).

The syntax of this command is as follows:

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

The keywords and arguments are as follows:

- **location** *name*—Geographical group name entities such as a city, data center, or content site for the location. Enter a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).

- **region** *name*—(Optional) Specifies a region with which the location will be associated. There should be a logical connection between the region and location. Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”).
- **comments** *text*—(Optional) Specifies descriptive information or important notes about the location. Enter up to 256 alphanumeric characters. Comments with spaces must be entered in quotes.
- **zone** *name*—(Optional) Specifies the name of an existing zone that is to be associated with the location. There should be a logical connection between the zone and the location.

To create a location named San_Francisco and associate it with the region Western_USA and the zone z1, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# location SAN_FRANCISCO region WESTERN_USA zone z1
```

To associate the zone “z3” with the location London, enter:

```
gssm1.example.com(config-gslb)# show gslb-config location
...
location London region Western_EU
...
gssm1.example.com(config-gslb)# location London zone z3
gssm1.example.com(config-gslb)#
```

Associating a Proximity-Based Location with an Answer

You can assign a location that is associated with a proximity zone to an answer by using the **answer vip** *ip_address* command in global server load-balancing configuration mode. You can make the association for a new answer or for an existing answer. To display a list of existing answers, use the **show gslb-config answer** command (see the “Displaying Answer Properties” section in Chapter 6, Configuring Answers and Answer Groups, for more information).

The syntax of this command is as follows:

answer vip *ip_address* [**name** *name* | **location** *name* | **active** | **suspend**]

The keywords and arguments are as follows:

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

To create a VIP answer called “SEC-LONDON1” and associate it with the “London” location, enter:

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

To associate the location Paris with the VIP answer called SEC-PARIS2, enter:

```
gssm1.example.com(config-gslb)# show gslb-config answer
...
answer vip 172.16.27.6 name SEC-PARIS2 active
          keepalive type tcp port 180 active
...
gssm1.example.com(config-gslb)# answer vip 172.16.27.6 name SEC-PARIS2 location Paris
gssm1.example.com(config-ansvip[ans-ip])
```

Configuring Proximity Using the Primary GSSM CLI

This section describes how to configure the GSS for network proximity from the primary GSSM CLI, how to add proximity to a DNS rule, and how to manage the proximity database. It contains the following topics:

- Configuring Proximity
- Creating DRP Keys
- Deleting DRP Keys
- Adding a Proximity Balance Clause to a DNS Rule
- Creating Proximity Groups
- Configuring Static Proximity Database Entries
- Deleting Entries from the Proximity Database
- Dumping Proximity Database Entries to a File
- Running a Periodic Proximity Database Backup
- Loading Proximity Database Entries

Configuring Proximity

The GSS contains proximity settings that function as the default values used by the GSS network when you enable proximity in a DNS rule.

You can enter the proximity properties configuration mode by using the **proximity-properties** command from global server load-balancing configuration mode. In the proximity properties configuration mode, enable proximity and modify the DNS proximity settings for the GSS network. Proximity settings are applied as soon as you exit from the proximity properties configuration mode or enter a new mode.

To enable proximity and configure the proximity settings from the proximity properties configuration mode, specify one or more of the following commands:

- **enable**—Enables global proximity across the entire GSS network. This command is disabled by default.
- **mask** *netmask*—Specifies a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses as an attempt to increase the number of supported D-proxies in the PDB. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). The default global mask is 255.255.255.255.

  When you define a proximity group for incoming D-proxy addresses, and an incoming D-proxy address does not match any of the entries in a defined proximity group, the GSS uses this global netmask value to calculate a grouped D-proxy network address. See the "Creating Proximity Groups" section for more information.

- **timeout** *minutes*—Specifies the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry. This value defines the PDB entry age-out process. Once an entry reaches the inactivity time, the GSS removes the selected dynamic entries from the PDB. Enter a value from 5 to 10080 minutes (168 hours). The default value is 4320 minutes (72 hours).
- **equivalence** *number*—Specifies a percentage that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Through the equivalence percentage, you define an RTT window that the GSS uses to consider zones equal. The equivalence value enables the GSS to prioritize between multiple distributed servers that have similar server-to-client RTT values. The GSS considers any RTT value that is less than or equal to the lowest RTT plus the percentage to be equivalent to the lowest RTT value. The GSS chooses one answer from a set of answers in equal zones.

  For example, with an equivalence setting of 20 percent and a series of returned RTT values:

  - Zone1 = RTT of 100 ms
  - Zone2 = RTT of 120 ms
  - Zone3 = RTT of 150 ms

  The GSS determines that Zone1 has the lowest RTT value. In this case, the GSS adds 20 percent (20 ms) to the RTT value to make Zone1 and Zone2 equally proximate in regards to the GSS selecting an answer. The RTT equivalence window range is 100 ms to 120 ms, and the GSS considers any zone that returns an RTT value in that range to be equally proximate.

  Use this parameter to adjust the granularity of the proximity decision process. Enter an equivalence value from 0 to 100 percent. The default value is 20 percent.
- **refresh-interval** *hours*—Specifies the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. Enter a value from 1 to 72 hours. The default value is 8 hours.
- **discovery-sequence—**Specifies either TCP or ICMP as the initial probe method used by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the router attempts the specified initial probe method and the D-proxy does not recognize the method, the GSS automatically chooses the other probe method to contact the D-proxy. Details about the probe methods are as follows:
  - **tcp**—The proximity probing agent uses the TCP SYN-ACK and RST handshake sequence to probe the user-specified TCP port and measure the RTT between the proximity probing agent and the D-proxy. You can configure the source and destination TCP ports on the router.
  - **icmp**—The proximity probing agent uses an ICMP echo request and response to measure the RTT between the proximity probing agent and the D-proxy.
- **fallback-probe-method path-probe**—Enables the path-probe method as the fallback method that the GSS (acting as a DRP agent) uses when both the TCP and ICMP probe methods fail.

  Note The GSS supports the path-probe method only when you have it configured as a DRP agent (see the "Configuring the GSS as a DRP Agent" section). By default, the path-probe method is not enabled.

  When the GSS fails to receive the minimum acceptable RTT metrics from the DRP agents, it sends a query message to the proximity probing agents configured for each zone instructing the DRP agent running on the GSS to probe using the path-probe method instead. If at least one of the DRP agents returns RTT using the legacy ICMP or 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 proximity probing agent and the D-proxy. The calculated path information is then sent back to the querying GSS.

The metrics obtained from the DRP agents configured for each zone are compared by the GSS to arrive at a common gateway. The best (smallest) RTT metric to the first common gateway is used to determine the closest content serving site. This method differs from the TCP and ICMP probe methods by calculating RTT to the common gateway, not to the D-proxy.

- **acceptable-rtt** *number*—Specifies a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. If the zones configured on the GSS report an RTT that is less than the specified acceptable-rtt value, the GSS does the following:
  a. Disregards the acceptable percentage of zones.
  b. Considers that there is sufficient proximity data to make a proximity decision.
  c. Uses the zones reporting less than or equal to this value in the proximity decision.

  Use this setting to adjust the granularity of the proximity decision process. Enter an acceptable-rtt value from 50 to 2000 ms. The default value is 100 ms.
- **acceptable-zone** *number*—Specifies a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The value specifies the percentage of all zones configured and used for a DNS rule and answer group. If an insufficient number of zones report RTT information, the balance clause fails and the GSS processes a new clause. For example, if the answer group associated with a clause includes answers that correspond to 5 different zones and you specify an acceptable-zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of 2 zones to satisfy the 40-percent criteria. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

  Use this parameter to adjust the granularity of the proximity decision process. Enter a percentage of zones from 3 to 100 percent. The default value is 40 percent.

Note If the reported RTT from one or more zones for the DNS rule/answer group is below the acceptable-rtt value, then the acceptable-zone value is ignored by the GSS.

- **wait enable/disable**—Instructs the GSS to wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process. In the disabled state (the default), the GSS does not wait to perform a proximity selection if it has not received the appropriate RTT and zone information based on other proximity settings. Instead, the GSS proceeds to the next balance clause in the DNS rule.
- **authentication drp enable**—Instructs the GSS to authenticate packets that it exchanges with the DRP agent in a proximity probing agent through the exchange of DRP keys (see the **key drp** command). The key authenticates the DRP requests and responses sent between the GSS and the DRP agent. In the disabled state (the default), the GSS does not perform DRP authentication with the DRP agent. See the "Creating DRP Keys" section for more information.
- **key drp**—If you enabled the **authentication drp enable** command (see above), create one or more DRP keys. Each DRP key contains a key identification number and a key authentication string. The primary GSSM supports a maximum of 32 keys.

Specify the following settings for the **key drp** command:

- *id_number*—The identification number of a secret key used for encryption. The GSS uses the ID value to retrieve the key string that is used to verify the DRP authentication field. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS. You can add a maximum of 32 keys. The range of key identification numbers is 0 to 255.
- *auth_string*—The authentication string that is sent and received in the DRP packets. The string must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The string can contain 1 to 80 uppercase and lowercase alphanumeric characters. However, the first character cannot be a number.

See the "Creating DRP Keys" section for more information.

To enable global proximity and specify settings, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# enable
gssm1.example.com(config-gslb-proxprop)# mask 255.255.255.0
gssm1.example.com(config-gslb-proxprop)# timeout 4320
gssm1.example.com(config-gslb-proxprop)# equivalence 20
gssm1.example.com(config-gslb-proxprop)# refresh-interval 6
gssm1.example.com(config-gslb-proxprop)# discovery-sequence icmp
gssm1.example.com(config-gslb-proxprop)# acceptable-rtt 100
gssm1.example.com(config-gslb-proxprop)# acceptable-zone 40
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

To reset various global proximity settings back to the default setting, use the **no** form of the command. For example, enter:

```
gssm1.example.com(config-gslb-proxprop)# no mask 255.255.255.0
gssm1.example.com(config-gslb-proxprop)# no timeout 4320
gssm1.example.com(config-gslb-proxprop)# no equivalence 20
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Creating DRP Keys

DRP supports the authentication of packets exchanged between the DRP agent (proximity probing agent) and the DRP client (the GSS). Use the **authentication drp enable** and **key drp** commands in proximity properties configuration mode to enable DRP authentication and create one or more DRP keys. See the "Configuring Proximity" section for details on these two commands. Each DRP key contains a key identification number and a key authentication string. The primary GSSM supports a maximum of 32 keys.

The DRP key is stored locally on each GSS in the network. The key functions as an encrypted password to help prevent DRP-based denial-of-service attacks, which can be a security threat. Each GSS generates DRP packets that contain all of the configured keys and sends the packets to the DRP agent in each configured zone. The DRP agent in each proximity probing agent examines the packet for a matching key (see the "Configuring the DRP Agent" section). If it finds a matching key, the DRP agent considers the DRP connection as authentic and accepts the packet.

To create three new DRP keys, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# authentication drp enable
gssm1.example.com(config-gslb-proxprop)# key drp 10 DRPKEY1
gssm1.example.com(config-gslb-proxprop)# key drp 20 DRPKEY2
gssm1.example.com(config-gslb-proxprop)# key drp 30 DRPKEY3
gssm1.example.com(config-gslb-proxprop)# exit
```

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

Deleting DRP Keys

You can remove DRP authentication keys by using the **no** form of the **key drp** command.

For example, enter:

```
gssm1.example.com(config-gslb-proxprop)# no key drp 30 DRPKEY3
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

Adding a Proximity Balance Clause to a DNS Rule

This section contains the following topics:

Proximity Balance Clause Overview

After you enable and configure network proximity from the primary GSSM, add proximity to a DNS rule for VIP-type answer groups using the **clause** command in rule configuration mode. The balance method configured in the matched clause of the DNS rule determines the answer that the GSS selects when multiple valid answers are present in the most proximate zones and returns this answer as the DNS response to the requesting D-proxy. If the GSS does not find an answer, it evaluates the other balance methods in the DNS rule to choose a new answer.

The GSS supports proximity in a DNS rule with the following balance methods:

- Ordered
- Round-robin
- Weighted-round-robin
- Least-loaded

You can configure proximity individually for the three balance clauses in a DNS rule. Proximity lookup occurs when the DNS rule is matched and the associated clause has the proximity option enabled. When the GSS receives a request from a D-proxy and decides that a proximity response should be provided, the GSS identifies the most proximate answer (the answer with the smallest RTT time) from the PDB residing in GSS memory and sends that answer to the requesting D-proxy. If the PDB is unable to determine a proximate answer, the GSS collects the zone-specific RTT results, measured from proximity probing agents in every zone in the proximity network, and puts the results in the PDB.

When there are no valid answers in the answer group of a proximity balance clause, the GSS skips that balance clause and moves on to the next clause listed in the DNS rule unless you specify a proximity wait condition. In that case, the GSS waits to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process.

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

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

To add proximity balance clauses to a DNS rule that uses VIP-type answer groups, perform the following steps:

1. If you have not already done so, configure and enable the global proximity settings. See the "Configuring Proximity" section for details.
2. Develop your DNS rule by using the **dns rule** command, as described in the "Building DNS Rules" section of Chapter 7, Building and Modifying DNS Rules.
3. Configure Balance Clause 1 by using the **clause** *number* **vip-group** *name* command in the rule configuration mode.

The syntax of this command is as follows:

clause *number* **vip-group** *name* [**method** {**round-robin** | **least-loaded** | **ordered** | **weighted-round-robin** | **hashed** {**domain-name** | **source-address** | **both**}} | **count** *number* | **proximity** {**enable** [**rtt** *number* | **wait** {**enable** | **disable**} **zone** *number*] | **disable**} | **ttl** *number*]

The keywords and arguments are as follows:

- *number*—Balance Clause number (1, 2, or 3). You can specify a maximum of three balance clauses that use VIP-type answers.
- **vip-group** *name*—Specifies the name of a previously created VIP-type answer group.

Note Ensure that the answers in the answer group that you specify are contained in locations that are tied to a zone.

- **method**—(Optional) Specifies the method type for each balance clause. Method types are as follows:
  - **round-robin—**The GSS cycles through the list of answers that are available as requests are received. This is the default.
  - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request.

    The least-loaded option is available only for VIP-type answer groups that use a KAL-AP or Scripted keepalive.
  - **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports numbering gaps in an ordered list.

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

  - **weighted-round-robin**—The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.
  - **hashed**—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group. Enter one of the following:

    domain-name—The GSS selects the answer based on a hash value created from the requested domain name.

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

    both—The GSS selects the answer based on both the source address and domain name.

- **count** *number*—(Optional) Specifies the number of address records (A-records) that you want the GSS to return for requests that match the DNS rule. The default is 1 record.
- **proximity**—(Optional) Specify **enable** or **disable**:
  - **enable**—Activates proximity for the clause. When you specify **enable**, the following options are available:

    rtt *number*—Changes the proximity-acceptable RTT for the balance clause to value that differs from the global proximity configuration. The GSS uses this value as the user-specified acceptable RTT when determining the most proximate answer. See the **acceptable-rtt** *number* option in the "Configuring Proximity" section for details. Enter an acceptable RTT value from 50 to 2000 ms. The default value is 100 ms.
  - **wait enable/disable**—Changes the proximity wait state to a setting that differs from the global proximity configuration. When enabled, the GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. When disabled, the GSS proceeds to the next balance clause in the DNS rule. See the **wait** option in the "Configuring Proximity" section for details.
  - **zone** *number*—Changes the proximity-acceptable zone percentage for the balance clause to a value that differs from the global proximity configuration. This option specifies the percentage of all zones configured and is used for a DNS rule and answer group. See the **acceptable-zone** option in the "Configuring Proximity" section for details.
  - **disable**—Deactivates proximity for the clause.
- **ttl** *number*—(Optional) Specifies the duration of time in seconds that the requesting DNS proxy caches the response sent from the GSS and considers it to be a valid answer. Valid entries are 0 to 604,800 seconds. The default is 20 seconds.

4. Repeat the configuration process for Balance Clauses 2 and 3 by using the **clause** command.

To set up Balance Clauses 1 and 2 with proximity for the previously created DNS rule named drule03, enter:

```
gssm1.example.com(config-gslb)# dns rule drule03
gssm1.example.com(config-gslb-rule[rule-name])# clause 1 vip-group ANSGRP-VIP-03 method
ordered proximity enable rtt 75 zone 50
gssm1.example.com(config-gslb-rule[rule-name])# clause 2 vip-group ANSGRP-VIP-03 method
least-loaded proximity enable rtt 125 zone 50
gssm1.example.com(config-gslb-rule[rule-name])#
```

Creating Proximity Groups

This section contains the following topics:

Proximity Group Overview

The primary GSSM supports the creation of proximity groups. A proximity group allows you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its PDB as a single entry. Instead of multiple PDB entries, the GSS uses only one entry in the PDB for multiple D-proxies. The GSS treats all D-proxies in a proximity group as a single D-proxy when responding to DNS requests with the most proximate answers. Requests from D-proxies within the same proximity group receive the RTT values from the database entry for the group.

You create proximity groups from the primary GSSM CLI to obtain better scalability of your configuration and to allow for easy proximity group creation through automated scripts. The primary GSSM supports a maximum of 5000 proximity groups. Each proximity group contains 1 to 30 blocks of IP addresses and subnet masks (in dotted-decimal format).

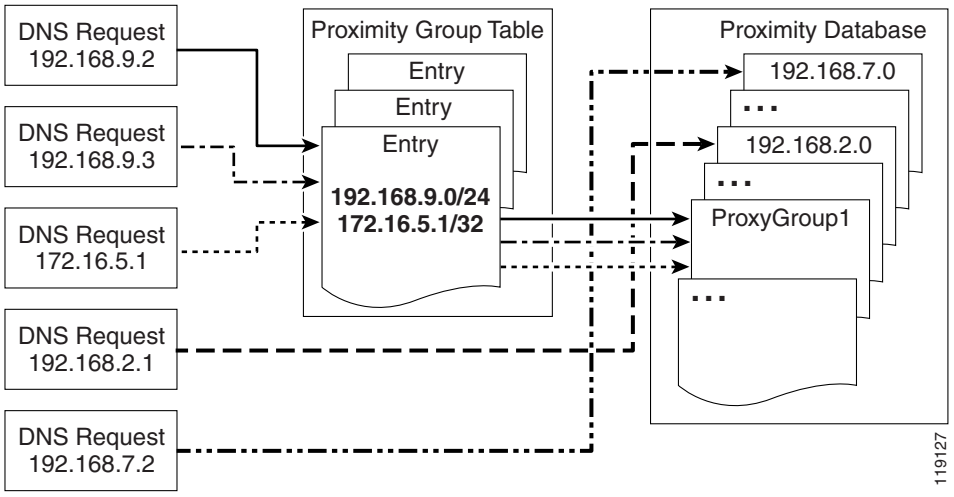
The benefits of proximity grouping are as follows:

- Fewer probing activities performed by the GSS which reduces the overhead associated with probing. The GSS probes the first requesting D-proxy from all configured zones to obtain the RTT value from each zone for the entire proximity group.
- Less space required for the PDB. Instead of multiple PDB entries, the GSS uses only one entry for multiple D-proxies.
- Greater flexibility in assigning alternative probing targets or static proximity metrics to a group.

In addition to creating proximity groups of multiple D-proxy IP addresses from the CLI, you can configure a global netmask from the primary GSSM to uniformly group contiguous D-proxies (see the "Configuring Proximity" section). The global netmask is used by the GSS device when no proximity group matches the incoming D-proxy address. The GSS uses the full incoming D-proxy IP address (255.255.255.255) and the global netmask as the key to look up the proximity database. The default global mask is 255.255.255.255.

Figure 9-3 shows how the DNS requests from D-proxies 192.168.9.2, 192.168.9.3, and 172.16.5.1 all map to the identified group name, ProxyGroup1, through proximity group entries 192.168.9.0/24 and 172.16.5.1/32. If no match is found in the PDB for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 9-3 Locating a Grouped Proximity Database Entry



Creating a Proximity Group

From the primary GSSM CLI, you can create a proximity group by using the **proximity group** global server load-balancing configuration mode command to identify the name of the proximity group and add an IP address block to the group. Use the **no** form of the command to delete a previously configured IP address block from a proximity group or to delete a proximity group.

Create proximity groups at the CLI of the primary GSSM to obtain better scalability of your configuration and to allow easy proximity group creation through automated scripts. Proximity groups are saved in the primary GSSM database. All GSS devices in the network receive the same proximity group configuration. You cannot create proximity groups at the CLI of a standby GSSM or individual GSS devices.

The syntax of this command is as follows:

proximity group {*groupname*} **ip** {*ip-address*} **netmas**k {*netmask*}

The keywords and arguments are as follows:

- *groupname*—Unique alphanumeric name. Names must have a maximum of 80 characters and spaces are not allowed.
- **ip** *ip-address*—Specifies the IP address block in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmas*k—Specifies the subnet mask of the IP address block in dotted-decimal notation (for example, 255.255.255.0).

To create a proximity group called ProxyGroup1 with an IP address block of 192.168.9.0 255.255.255.0, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity group ProxyGroup1 ip 192.168.9.0 netmask
255.255.255.0
```

Reenter the **proximity group** command if you want to perform the following:

- Add multiple IP address blocks to a proximity group

- Create additional proximity groups

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

Playing Static Proximity Group Configurations

If the size of static proximity group configuration is quite large, you should use the **proximity play-config** command to play the static proximity configuration. This command plays the proximity commands more efficiently than **script play-config**.

Note This command is only supported on the primary and secondary GSSM.

The syntax of this command is as follows:

proximity play-config *filename*

The *filename* specifies the file containing the proximity configuration.

To use this command, perform the following steps:

1. Ensure that the primary and secondary GSSMs are synchronized.
2. Stop the primary GSSM by entering the **gss stop** command.
3. Enter **proximity play-config** in privileged EXEC mode.
4. Bookmark the key that is generated after you enter the command.
5. Stop the secondary GSSM by entering the **gss stop** command.
6. Enter **proximity play-config** in privileged EXEC mode.
7. Enter the key generated from the primary GSSM at the prompt.

Note You should ensure that the secondary GSSM is registered to the primary before entering **proximity play-config** on the primary GSSM.

To play a static proximity configuration, enter:

```
gssm1.example.com# proximity play-config prox.txt
Tue Mar 6 13:10:43 2007 waiting for postmaster to start....done
Tue Mar 6 13:10:43 2007 postmaster successfully started
proximity group proxa1 ip 11.1.1.4 netmask 255.255.255.252
proximity group proxa1 ip 11.1.1.8 netmask 255.255.255.252
.
.
.
proximity group proxa50 ip 11.1.2.140 netmask 255.255.255.252
proximity group proxa50 ip 11.1.2.144 netmask 255.255.255.252
##########################################
Please use the following Key required while, playing "proximity play-config" on SGSSM.
Key: 8912515fa7339c1b60a20b60142493328b997b
##########################################
```

Deleting a Proximity Group IP Address Block

You can delete a previously configured IP address block from a proximity group by using the **no** form of the **proximity group** command. For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no proximity group ProxyGroup1 IP 192.168.9.0 netmask
255.255.255.0
```

Deleting a Proximity Group

You can delete a proximity group and all configured IP address blocks by using the **no** form of the **proximity group** command. For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no proximity group ProxyGroup1
```

Configuring Static Proximity Database Entries

This section describes how to configure static entries in the PDB. It contains the the following topics:

- Adding Static Proximity Entries
- Static Entries and the Aging-Out Process
- Deleting Static Entries from the Proximity Database

Adding Static Proximity Entries

In the PDB, entries can be both dynamic and static. The GSS creates dynamic entries in the PDB as the result of requests from new D-proxy IP addresses. If you need to configure static proximity metrics for zones in your GSS network or assign proximity probing agents to specific D-proxies, you must define a series of static entries in the PDB by using the **proximity assign** global server load-balancing configuration mode command. If the same entry, dynamic or static, already exists in the proximity database, the GSS will overwrite that entry with the newly-assigned entry. You can use automated scripts if you intend to add numerous static entries in the PDB of each GSS.

You can also successfully add static proximity entries on the primary GSS. However, you cannot add entries by zone on any other GSS. When you attempt to use static entries locally and configure them separately on each GSS using the **proximity assign** CLI command, the GSS responds that this command is valid only on the primary GSSM.

Note Be aware that the **proximity assign** CLI command affects only the local GSS. The configuration is not synchronized with the other GSSs in the network.

There are two different keywords and arguments to consider here when using the **proximity assign** command:

- **proximity assign ip** *entryaddress* is supported on all GSSs. Thus, if you want to add the same static entries in the PDBs of the other GSS devices in your network, enter **proximity assign ip** *entryaddress* at the CLI of each GSS.

- **proximity assign group** *groupname* is supported only on the primary GSSM, as is configuring the **proximity group** command. Proximity group configurations are synchronized with all other GSSs in the network once they register with the primary GSSM and are activated.

  For more information on these and all other **proximity assign** keywords and arguments, see the "Static Entries and the Aging-Out Process" section.

  To synchronize the proximity static entries for the group round-trip time (RTT) data, perform the following steps.

  1. On the primary GSSM, back up the static proximity entries of the primary GSSM to a sample file named PDB2007_6_21 as follows:

     ```
     gss-primary.example.com# proximity database dump PDB2007_6_21 format binary
     entry-type assigned
     ```

  2. You should then transfer the sample PDB2007_6_21 file from the primary to the other GSS. To do so, use FTP to perform the file download on the other GSS as follows:

     ```
     gss-other.example.com# ftp <primary_GSS_ipaddress>
     ```

     Note Before performing this step, ensure that the FTP service is enabled on the primary GSS.

  3. On any other GSS, load the primary GSSM's static proximity entries from a sample file named PDB2007_6_21 as follows:

     ```
     gss1.example.com# proximity database load PDB2007_6_21 format binary
     ```

Static Entries and the Aging-Out Process

Static entries in the PDB do not age out; they remain in the PDB until you delete them. Static entries are not subject to the automatic database cleanup of least recently used entries when the PDB size is almost at the maximum number of entries. Use the **no proximity assign** command to delete static entries as described in the "Deleting Static Entries from the Proximity Database" section.

You can specify permanent RTT values for the static entries. When the GSS uses permanent RTT values, it does not perform active probing with the DRP agent. Instead of RTT values, you can specify alternative IP addresses as targets for probing by the proximity probing agents to obtain RTT data. The GSS probes the alternative probe target for requests from D-proxies matching these static entries.

Static entries in the PDB are either static RTT-filled or probe-target IP-filled.

You can create static entries in the PDB by using the **proximity assign** global server load-balancing configuration mode command.

The syntax of this command is as follows:

proximity assign {**group** {*groupname*}} | **ip** {*entryaddress*} | [**probe-target** {*ip-address*} | **zone-data** {"*zoneId:RTT*"}]

Note The GSS accepts commands up to 1024 characters. Ensure that the **proximity assign** command does not exceed that length when you configure RTT for a large number of proximity zones.

The options and variable are as follows:

- **group** *groupname*—Specifies a unique alphanumeric name with a maximum of 80 characters. Names that include spaces must be entered in quotes (for example, “name 1”). Each static proximity group must have a unique name.
- **ip** *entryaddress*—Specifies the D-proxy IP address entry to be created in the PDB.
- **probe-target** *ip-address*—(Optional) Specifies an alternate IP address for the proximity probing agent to probe. Normally, the proximity probing agent transmits a probe to the requesting D-proxy IP address to calculate RTT. If you find that the D-proxy cannot be probed from the proximity probing agent, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.
- **zone-data** “*zoneId:RTT*”—(Optional) Specifies the calculated RTT value for a zone, specified in “*zoneId:RTT*” format. For example, enter **“1:100”** to specify zone 3 with an RTT of 100 seconds. Valid entries for *zoneID* are 1 to 32, and must match the proximity zone index specified through the primary GSSM (see the “Synchronizing the GSS System Clock with an NTP Server” section). Valid entries for the *RTT* value are 0 to 86400 seconds (1 day). To specify multiple static *zone:RTT* pairs in the proximity group, separate each entry within the quotation marks by a comma, but without spaces between the entries (for example, “3:450,22:3890,31:1000”).

To configure an alternative probing target for the proximity group ISP1, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP1 probe-target 192.168.2.2
```

To configure an alternative probing target for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0), enter:

```
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
```

To configure static RTT metrics for the proximity group ISP2 using zone indexes created previously through the primary GSSM, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign group ISP2 zone-data
"1:100,2:200,3:300,4:400,5:500"
```

To configure static RTT metrics for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0), enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign ip 192.168.8.0 zone-data
"1:100,2:200,3:300,4:400,5:500"
```

Deleting Static Entries from the Proximity Database

The GSS allows you to remove entries from the PDB of each GSS device using the CLI. To delete static entries from the PDB in the GSS memory, use the **no** form of the **proximity assign** global server load-balancing configuration mode command.

Note Ensure that you want to permanently delete static entries from the PDB before you enter the **no proximity assign** command. You cannot retrieve those static entries once they are deleted.

To delete static RTT entries for the proximity group ISP1, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no proximity assign group ISP1 zone-data
"1:100,2:200,3:300,4:400,5:500"
```

Deleting Entries from the Proximity Database

You can remove PDB entries from the GSS memory by using the **proximity database delete** command. This command, however, does not delete PDB entries saved as part of an automatic dump to a backup file on disk, which the GSS loads upon a reboot or restart to initialize the PDB. To ensure that you successfully remove the desired PDB entries from both GSS memory and disk, enter the **proximity database delete** command followed by the **proximity database periodic-backup now** command to force an immediate backup of the empty PDB residing in GSS memory.

The syntax of this command is as follows:

proximity database delete {**all** | **assigned** | **group** {*name*} | **inactive** *minutes* | **ip** {*ip-address*} **netmask** {*netmask*} | **no-rtt** | **probed**}

The keywords and arguments are as follows:

- **all**—Removes all proximity database entries from the GSS memory. The prompt "Are you sure?" appears to confirm the deletion of all PDB entries. Specify **y** to delete all entries or **n** to cancel the deletion operation.

Caution Use the **proximity database delete all** command when you want to remove all entries from the PDB and empty the database. Ensure that you want to permanently delete entries from the PDB before you enter this command since you cannot retrieve PDB entries once you delete them.

- **assigned**—Removes all static entries from the PBD.
- **group** *name*—Removes all entries that belong to a named proximity group. Specify the exact name of a previously created proximity group.
- **inactive** *minutes*—Removes all dynamic entries that have been inactive for a specified time. Valid values are 0 to 43200 minutes.
- **ip** *ip-address* **netmask** *netmask*—Removes all proximity entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **no-rtt**—Removes all entries from the PDB that do not have valid RTT values.
- **probed**—Removes all dynamic entries from the PDB.

To remove the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

```
gssm1.example.com# proximity database delete ip 192.168.8.0 255.255.255.0
```

Dumping Proximity Database Entries to a File

The GSS automatically dumps PDB entries to a backup file on the disk approximately every hour. The GSS uses this backup file to initialize the PDB upon system restart or reboot to enable the GSS to recover the contents of the database.

You can dump all or selected entries from the PDB to a named file as a user-initiated backup file. You can then use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the file to a remote machine.

To view the entire contents of a PDB XML output file from the GSS, use the **type** command. See the *Cisco Global Site Selector Administration Guide* for details about displaying the contents of a file.

The GSS includes options that provide a level of granularity for dumping entries from the PDB. The GSS supports binary and Extensible Markup Language (XML) output formats. Optionally, you can specify filters, such as PDB entry type and entry IP network address, to clarify the information dumped from the PDB. PDB entry types can be either statically entered (see the "Configuring Static Proximity Database Entries" section) or dynamically learned by the GSS. You can instruct the GSS to dump both type of entries from the PDB. If you do not specify an entry type, the GSS automatically dumps all entries from the PDB.

If you attempt to overwrite an existing proximity database dump file with the same filename, the GSS displays the following message:

Proximity Database dump failed, a file with that name already exists.

You can dump entries contained in the PDB to a named file by using the **proximity database dump** command.

The syntax of this command is as follows:

proximity database dump {*filename*} **format** {**binary** | **xml**} [**entry-type** {**all** | **assigned** | **probed**}] [**entry-address** {*ip-address*} **netmask** {*netmask*}]

The keywords and arguments are as follows:

- *filename*—Name of the output file that contains the PDB entries on the GSS disk. This file resides in the /home directory.
- **format**—Dumps the PDB entries in binary or XML format. Choose binary encoding as the format type if you intend to load the contents of the file into the PDB of another GSS. The valid entries are as follows:
  - **binary**—Dumps the assigned proximity entries in true binary format. This file can be used only with the proximity database load command
  - **xml**—Dumps the assigned proximity entries in XML format. The contents of an XML file include the data fields and the data descriptions. The contents of this file can be viewed using the **type** command. See Appendix B, "Sticky and Proximity XML Schema Files" for information on defining how content appears in output XML files.

Note Dumping PDB entries in XML format can be a resource intensive operation and may take from 2 to 4 minutes to complete depending on the size of the PDB and the GSS platform in use. To avoid a degradation in performance, we recommend that you do not perform a PDB dump in XML format during the routine operation of the GSS.

- **entry-type**—Specifies the type of PDB entries to output: static, dynamic, or both. The valid entries are as follows:

  - **all**—Dumps static and dynamic entries from the PDB. This is the default.
  - **assigned**—Dumps statically assigned proximity entries.
  - **probed**—Dumps dynamically probed proximity entries.
- **entry-address** *ip-address*—Specifies the IP address of the PDB entry.
- **netmask** *netmask*—Specifies the subnet mask of the PDB entry in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to dump the dynamic PDB entries to a file named PDB2004_6_30 in XML format. If the dump contains a large number of entries, progress messages may appear.

```
gssm1.example.com# proximity database dump PDB2004_6_30 format xml entry-type probed
entry-address 172.23.5.7 netmask 255.255.255.255
Starting Proximity Database dump.

gssm1.example.com# proximity database dump PDB2004_6_30 format xml entry-type probed
entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump is in progress...
Proximity Database has dumped 15678 of 34512 entries

gssm1.example.com# proximity database dump PDB2004_6_30 format xml entry-type probed
entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump completed. The number of dumped entries: 34512
```

When the dump finishes, a "completed" message displays and the CLI prompt reappears.

Running a Periodic Proximity Database Backup

You can instruct the GSS to dump PDB entries to an output file on the GSS disk before the scheduled time. You may want to initiate a PDB dump as a database recovery method to ensure you store the latest PDB entries before shutting down the GSS.

You can force an immediate backup of the PDB residing in GSS memory by using 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 of this command is as follows:

proximity database periodic-backup now

For example, enter:

```
gssm1.example.com# proximity database periodic backup now
```

Loading Proximity Database Entries

The GSS enables you to load and merge a PDB from a file into the existing PDB in GSS memory. This PDB merge capability supports the conversion and migration of PDB entries from one GSS into the PDB of another GSS. The file must be in binary format for loading into GSS memory. Proximity RTT metrics loaded from the file replace overlapping entries that exist in the database and supplement the nonoverlapping database entries.

You can load a PDB from disk into GSS memory by using the **proximity database load** command.

The syntax of this command is as follows:

proximity database load *filename* **format binary** [**override**]

The keywords and arguments are as follows:

- *filename*—Name of the PDB file to load and merge with the existing PDB on the GSS device. The file must be in binary format for loading into the GSS memory (see the "Dumping Proximity Database Entries to a File" section). Use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the PDB file to the GSS from a remote GSS.
- **format binary**—Loads the assigned proximity file in true binary format. The file must be in binary format to be loaded into GSS memory.
- **override**—(Optional) Specifies if the proximity database entries in the file are to override the same entries located in the current GSS PDB. When you choose the **override** option, static database entries always have priority over dynamic database entries in the PDB. For the same database entries that exist in both the file and in GSS database memory, the GSS does the following:
  - Overwrites dynamic entries with any overlapping static entries
  - Overwrites static entries with any overlapping static entries, but does not overwrite those entries with any overlapping dynamic entries

  If you do not specify the **override** option, the GSS loads the most recent entries into memory, which will replace the older entries of the same type (dynamic or static) in the PDB. For example, the most recent dynamic entries replace the older dynamic entries in the PDB.

To load the entries from the GSS3PDB file without overriding the existing entries in the GSS PDB, enter:

```
gssm1.example.com# proximity database load file GSS3PDB format binary
```

To override the same entries located in the existing GSS PDB, enter:

```
gssm1.example.com# proximity database load GSS3PDB format binary override
```

Initiating Probing for a D-proxy Address

The GSS sends a probe request to each configured probe device in a specified zone to obtain probe information (RTT values). The GSS uses the obtained probe information from the D-proxy to update the PDB entry if the entry can be found in the PDB.

You may need to instruct the proximity probing agent in one or all zones (broadcast) to send a probe to a specific D-proxy address, obtain an RTT value, and save the entry in the PDB. You can initiate direct probing to a specific D-proxy IP address or direct probing to one or more zones by using the **proximity probe** command.

The syntax of this command is as follows:

proximity probe {*dproxy_address*} [**zone** {*zoneId* | **all**}]

The keywords and arguments are as follows:

- *dproxy_address*—IP network address of the D-proxy that you want to probe from the proximity probing agent.
- **zone** *zoneId*—Specifies the ID of the proximity zone that contains the proximity probing agent from which you want to initiate a probe. Available values are 1 to 32.
- **all**—Specifies that the GSS instruct the proximity probing agents in all configured zones to transmit a probe to the specified D-proxy IP address.

To instruct the proximity probing agent in zone 1 to send a probe to the D-proxy at 172.16.5.7, enter:

```
gssm1.example.com# proximity probe 172.16.5.7 zone 1
```

Disabling Proximity Locally on a GSS for Troubleshooting

You can disable proximity for a single GSS when you need to locally override the globally-enabled proximity option to troubleshoot or debug the device.The GSS does not store the local disable setting in its running-config file.

When you enter the **proximity stop** command, the GSS immediately stops the following operations:

- Proximity lookups in the PDB
- Direct probing between the GSS and DRP agents
- Refresh probing to obtain the most up-to-date RTT values
- Periodic PDB dumps
- The proximity database entry age-out process

When you restart the device, the GSS reenables network proximity.

To locally disable proximity on a GSS device using the **proximity stop** command, enter:

```
gssm1.example.com# proximity stop
```

To locally reenable proximity on a GSS device using the **proximity start** command, enter:

```
gssm1.example.com# proximity start
```

Where to Go Next

Chapter 10, Configuring DDoS Prevention, describes how to configure a GSS to prevent Distributed Denial of Service attacks.