Configuring Network Proximity

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

This chapter contains the following major sections:

- Network Proximity Overview
- Proximity Network Design Guidelines
- Network Proximity Quick Start Guide
- Configuring a Cisco Router as a DRP Agent
- Synchronizing the GSS System Clock with an NTP Server
- Creating Zones Using the Primary GSSM CLI
- Configuring Proximity Using the Primary GSSM CLI
- Initiating Probing for a D-proxy Address
- Disabling Proximity Locally on a GSS for Troubleshooting

Each GSS supports a comprehensive set of **show** CLI commands to display network proximity statistics for the device. In addition, the primary GSSM GUI displays statistics about proximity operation for the GSS network. Refer to Chapter 12, 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. In this context, proximity refers to the distance or delay in terms of network topology, not geographical distance, between the requesting client's D-proxy and its answer.

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

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

This section describes the major functions in GSS network proximity:

- Proximity Zones
- Probe Management and Probing
- Proximity Database
- Example of Network Proximity

Proximity Zones

A network can be logically partioned into "zones" based on the arrangement of devices and network partioned characteristics. A zone can be geographically related to data centers in a continent, a country, or a major city. All devices, such as web servers in a data center, that are located in the same zone have the same proximity value when communicating with other areas of the Internet.

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

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

Probe Management and Probing

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

The GSS uses Director Response Protocol (DRP) to communicate with the probing devices (called DRP agents) in each zone. DRP is a general User Datagram Protocol (UDP)-based query and response information exchange protocol developed by Cisco Systems. You can use any Cisco router as the probing device in a zone that is capable of supporting the DRP agent software and can measure ICMP or TCP RTT. The GSS communicates with the Cisco IOS-based router using the DRP RTT query and response method.

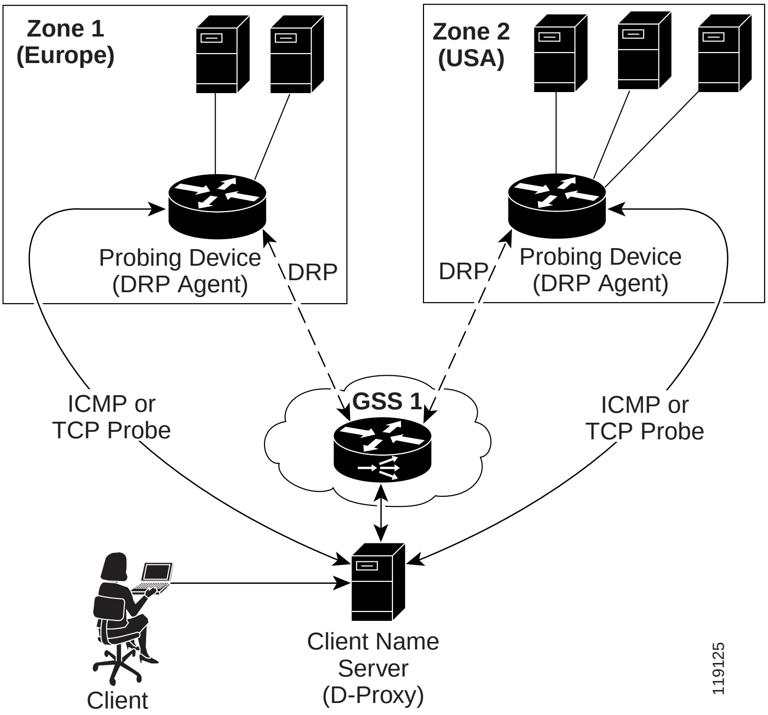
Each DRP agent accepts probing instructions from the GSS and returns probing results to the GSS based on the DRP protocol. DRP allows for the authentication of packets exchanged between the DRP agent and the GSS.

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

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

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

Figure 9-1 DRP Communication in a GSS Network



The GSS supports two type of probing methods:

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

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

Proximity Database

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

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

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

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

The GSS supports a maximum of 500,000 D-proxy IP address entries in the PDB table, 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 required, you can add static entries to the PDB by specifying permanent RTT values (gathered by other means), and optionally, alternative IP addresses to probe.

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

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

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

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

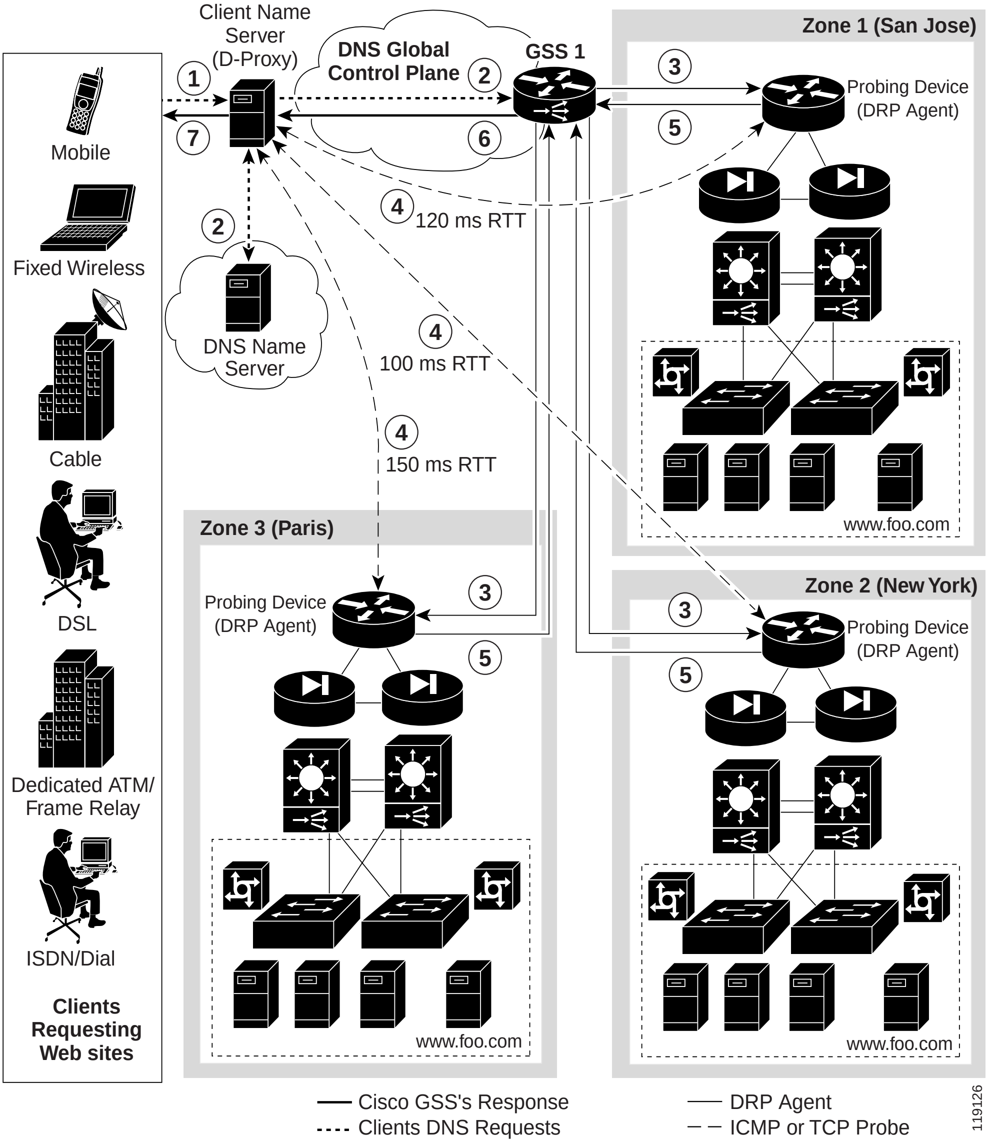
When the PDB reaches a maximum of 500,000 entries, the GSS does not add entries to the PDB and any new requests for answers result in a failure. The GSS tracks how many entries are dropped when the maximum limit has been reached. Once the number of PDB entries drops below 500,000, the GSS resumes adding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

Example of Network Proximity

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

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

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



Proximity Network Design Guidelines

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

- Decide how many zones you require for your proximity network based on your current network configuration and the level of proximity that you require for your network. A maximum of 32 zones is allowed within each GSS proximity environment. You can change zone configuration at any time by deleting or adding a zone, or by moving a zone from one location to another location.
- For each zone, identify the probing device and optionally the back up the probing device. Each probing device represents the topological location of its associated zone and also reflects the zone's expected network behavior in terms of connectivity to the internet. The probing device is the DRP agent located within the zone.
- Each GSS network can contain a maximum of eight GSS devices. You can add or delete GSS devices at any time. The GSS does not have to reside within a zone.
- To use proximity, you must:
  - Associate a proximity zone with a location
  - Assign a location that is associated with a proximity zone to an answer

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

Network Proximity Quick Start Guide

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

Table 9-1 Proximity Configuration Quick Start

Task and Command Example

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

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

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

4. Use the **zone** command to configure a proximity zone from the primary GSSM.
For example:
`gssm1.example.com(config-gslb)# zone Z1 index 1 probe`
`192.168.11.1 backup probe 192.168.11.5`

5. Use the **proximity-properties** command in global server load-balancing configuration mode to enter the proximity properties configuration mode.
For example:
`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:
`gssm1.example.com(config-gslb-proxprop)# enable`
`gssm1.example.com(config-gslb-proxprop)# exit`
`gssm1.example.com(config-gslb)#`

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
7. Configure global proximity configuration default settings using the following commands in proximity properties configuration mode. Refer to the "Configuring Proximity" section for a complete description of these settings. You can configure: • **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). • **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) used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the Cisco router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically chooses a different probe method to contact the D-proxy. • **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.

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) To enable DRP authentication and create a DRP key, use 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 wish 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)#
```

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

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 using the **dns rule** command.

    For example:

    ```
    gssm1.example.com(config)# gslb
    gssm1.example.com(config-gslb)# dns rule drule03 owner
    WEB-SERVICES source-address-list WEB-GLOBAL-LISTS domain-list
    E-COMMERCE query A
    gssm1.example.com(config-gslb-rule[rule-name])#
    ```

12. Use the **clause** command to configure balance clause 1 for the DNS rule and the **proximity enable** option to enable proximity for the DNS rule.

    For example:

    ```
    gssm1.example.com(config-gslb-rule[rule-name])# clause 1
    vip-group method ordered ANSGRP-VIP-03 proximity enable
    gssm1.example.com(config-gslb-rule[rule-name])#
    ```

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

13. (Optional) Modify other **clause** command settings for proximity as appropriate. Refer to 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*—To change the proximity-acceptable RTT for the balance clause to a different value from the global proximity configuration, use this option.
    - **wait enable/disable** —To change the proximity wait state to a different setting than the global proximity configuration.
    - **zone** *number*—To change the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration, use this option.

    For example, to set up balance clause 1 with proximity for the previously created DNS rule named drule03, 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 clause 2.

    For example:

    ```
    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 clause 3, then repeat steps 12 and 13.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example

16. (Optional) To group multiple D-proxy IP addresses as a single entry in the PDB to reduce probing and to take up less space in the PDB, access the global server load-balancing configuration mode and create a proximity group at the primary GSSM. Use the **proximity group** command to add multiple D-proxy IP addresses and subnet masks to the group.

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

17. (Optional) To add static proximity entries to the PDB of a GSS device in your network, access the global server load-balancing configuration mode and use the **proximity assign** command to create the static entries.

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

Configuring a Cisco Router as a DRP Agent

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

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

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

Choosing a Cisco Router as a DRP Agent

When selecting a Cisco router as the DRP agent in a zone, ensure that the:

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

Configuring the DRP Agent

To configure and maintain the DRP agent in the Cisco IOS-based router, perform the tasks described in the “Configuring IP Services” chapter, the “Configuring a DRP Server Agent” section, of the *Cisco IOS IP Configuration Guide*. The Cisco IOS-based router must support the DRP protocol in a proximity zone. DRP is supported in the following Cisco IOS release trains: 12.1, 12.1E, 12.2T, 12.2, 12.3, and later releases. ICMP probing is only supported in Cisco IOS release 12.2T, 12.3, and later.

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

The following procedure summarizes the steps required to configure a Cisco IOS-based router as a DRP agent:

1. Enable the DRP agent in the Cisco router.
2. Enable security for DRP by defining a standard access list that permits requests from 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 originating from an IP address in the list. If no access list is configured, the DRP agent answers all queries.
3. Ensure that the router accepts DRP queries from the IP addresses associated with 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 Cisco router running IOS release 12.1, it is important to ensure the DRP authentication configuration is identical on both devices. For example, if you intend to perform DRP authentication between a GSS and a Cisco IOS 12.1 router, ensure that you properly enable and configure authentication on both devices. The same is true if you choose not to use DRP authentication; disable authentication on both devices.If you disable DRP authentication on a Cisco IOS 12.1 router but enable DRP authentication on a GSS, all measurement probes sent by a GSS to the Cisco IOS-based router will fail. This condition occurs because the Cisco IOS 12.1 router fails to recognize the DRP echo query packets sent by a GSS and the GSS cannot detect a potential failure of measurement packets sent to the router. In this case, the GSS identifies the Cisco IOS-based router as being ONLINE in its **show statistics proximity probes detailed** CLI command, yet the measurement response packets monitored in the Measure Rx field do not increment. Together, these two conditions may indicate a DRP authentication mismatch.

If DRP probe requests fails between the GSS and a Cisco router running IOS release 12.1, even when the GSS indicates that the router is ONLINE, verify the DRP authentication configurations on both the GSS and the Cisco router. To verify the DRP authentication configuration on the:

- Cisco router running IOS release 12.1, enter the **show ip drp** command. If the line `Authentication is enabled, using "test" key-chain` appears in the output (where `"test"` is the name of your key-chain), DRP authentication is configured on the router. If this line does not appear in the output, DRP authentication is not configured.
- 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 Cisco router running 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. Refer to the *Cisco Global Site Selector Administration Guide* for information on creating and managing user accounts.

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

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

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

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

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

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

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

Synchronizing the GSS System Clock with an NTP Server

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

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

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

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

Use the **ntp-server** global configuration mode command to specify one or more NTP servers for GSS clock synchronization. The syntax for this CLI command is:

ntp-server *ip_or_host*

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

Use the **ntp enable** global configuration mode command to enable the NTP service. The syntax of this CLI command is:

ntp enable

This example shows how to specify the IP addresses of two NTP time servers for a GSS device and to enable the NTP service:

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

Creating Zones Using the Primary GSSM CLI

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

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

This section includes the following procedures:

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

Configuring a Proximity Zone

To configure a proximity zone from the primary GSSM, use the **zone** command in global server load-balancing configuration mode.

The syntax of this command is:

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

The options for this command are:

- *name*—Specifies the 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 servicing 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 servicing 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), 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

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

The syntax for the **location** command is:

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

The variables and options for this command are:

- **location** *name*—Specifies a 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**—(Optional) Specifies descriptive information or important notes about the location. Enter up to 256 alphanumeric characters. Comments with spaces must be entered in quotes.

- **zone** *name*—(Optional) Specifies the name of an existing zone that is to be associated with the location. There should be a logical connection between the zone and the location.

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

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

To associate the zone "z3" with the location London, enter:

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

Associating a Proximity-Based Location with an Answer

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

The syntax of the **answer vip** command is:

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

The variables and options for this command are:

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

- **active**—(Optional) Reactivates a suspended VIP answer. This is the default setting.
- **suspend**—(Optional) Suspends an active VIP answer.

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

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

To 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 discusses how to configure the GSS for network proximity operation from the primary GSSM CLI, how to add proximity to a DNS rule, and how to manage the proximity database. It includes the following procedures:

- 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
- Dumping Proximity Database Entries to a File
- Running a Periodic Proximity Database Backup
- Loading Proximity Database Entries

Configuring Proximity

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

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

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

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

  When you define a proximity group for incoming D-proxy addresses, and an incoming D-proxy address does not match any of the entries in a defined proximity group, then 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 1 to 10080 minutes (168 hours). The default value is 4320 minutes (72 hours).

- **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. 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 Zone 1 and 2 equally proximate in regards to the GSS selecting an answer. The RTT equivalence window range is 100 ms to 120 ms, and the GSS considers any zone that returns an RTT value in that range to be equally proximate.

  Use this parameter to adjust the granularity of the proximity decision process. Enter an equivalence value from 0 to 100 percent. The default value is 20 percent.

- **refresh-interval** *hours*—Specifies the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. Enter a value from 1 to 72 hours. The default value is 8 hours.

- **discovery-sequence—**Specifies the type of probe method used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the Cisco router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically chooses a different probe method to contact the D-proxy. The available choices for the initial probe method are ICMP and TCP.

  – **tcp**—The probing device uses the TCP SYN-ACK and RST handshake sequence to probe the user-specified TCP port and measure the RTT between the probing device and the D-proxy. You can configure the source and destination TCP ports on the Cisco router.

  - **icmp**—The probing device uses ICMP echo request and response to measure the RTT between the probing device and the D-proxy.

- **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:

  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 500 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 five different zones and you specify an acceptable-zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of two zones to satisfy the 40 percent criteria. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

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

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

- **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. In this case, the GSS proceeds to the next balance clause in the DNS rule.
- **authentication drp enable—**Instructs the GSS to authenticate packets that it exchanges with the DRP agent in a probing device through the exchange of DRP keys (see **key drp** command listed below). The key authenticates the DRP requests and responses sent between the GSS and the DRP agent. In the disabled state (the default), the GSS does not perform DRP authentication with the DRP agent. See the "Creating DRP Keys" section for more information.
- **key drp**—If you enabled the **authentication drp enable** command (see above), create one or more DRP keys. Each DRP key contains a key identification number and a key authentication string. The primary GSSM supports a maximum of 32 keys.

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

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

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

For example, to enable global proximity and specify settings, enter:

```
gssm1.example.com(config-gslb)# proximity-properties
gssm1.example.com(config-gslb-proxprop)# enable
gssm1.example.com(config-gslb-proxprop)# mask 255.255.255.0
gssm1.example.com(config-gslb-proxprop)# timeout 4320
gssm1.example.com(config-gslb-proxprop)# equivalence 20
```

```
gssm1.example.com(config-gslb-proxprop)# refresh-interval 6
gssm1.example.com(config-gslb-proxprop)# discovery-sequence icmp
gssm1.example.com(config-gslb-proxprop)# acceptable-rtt 100
gssm1.example.com(config-gslb-proxprop)# acceptable-zone 40
gssm1.example.com(config-gslb-proxprop)# exit
gssm1.example.com(config-gslb)#
```

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

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

Creating DRP Keys

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

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

For example, to create three new DRP keys, enter:

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

Deleting DRP Keys

To remove DRP authentication keys, use 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 includes the following topics:

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

Proximity Balance Clause Overview

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

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

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

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

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

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

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

To add proximity balance clauses to a DNS rule that uses VIP-type answer groups:

1. If you have not already done so, configure and enable global proximity settings. See the "Configuring Proximity" section for details.
2. Develop your DNS rule 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 using the **clause** *number* **vip-group** *name* command in the rule configuration mode. The syntax for this command is:

   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 variables and options for this command are:

- *number*—Specifies the 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:
  - **round-robin—**The GSS cycles through the list of answers that are available as requests are received. This is the default setting.
  - **least-loaded**—The GSS selects an answer based on the load reported by each VIP in the answer group. The answer reporting the lightest load is chosen to respond to the request.The least-loaded option is available only for VIP-type answer groups that use a KAL-AP keepalive.
  - **ordered**—The GSS selects an answer from the list based on precedence; answers with a lower order number are tried first, while answers further down the list are tried only if preceding answers are unavailable to respond to the request. The GSS supports gaps in numbering in an ordered list.

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

  - **weighted-round-robin—**The GSS cycles through the list of answers that are available as requests are received but sends requests to favored answers in a ratio determined by the weight value assigned to that resource.

  - **hashed**—The GSS selects the answer based on a unique value created from information stored in the request. The GSS supports two hashed balance methods. The GSS allows you to apply one or both hashed balance methods to the specified answer group. Enter one:
    - **source-address**—The GSS selects the answer based on a hash value created from the source address of the request.
    - **domain-name**—The GSS selects the answer based on a hash value created from the requested domain name.
    - **both**—The GSS selects the answer based on both 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 a different value from the global proximity configuration. The GSS uses this value as the user-specified acceptable RTT when determining the most proximate answer. Refer to the **acceptable-rtt** *number* option in "Configuring Proximity" for details. Enter an acceptable RTT value from 50 to 500 ms. The default value is 100 ms.
    - **wait enable/disable —**Changes the proximity wait state to a different setting than 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. Refer to the **wait** option in "Configuring Proximity" for details.
    - **zone** *number*—Changes the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration. This option specifies the percentage of all zones configured and is used for a DNS rule and answer group. Refer to the **acceptable-zone** option in "Configuring Proximity" 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. Using the **clause** command, repeat the configuration process for clauses 2 and 3.

For example, to set up balance clauses 1 and 2 with proximity for the previously created DNS rule named drule03, enter:

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

Creating Proximity Groups

This section includes the following topics:

- Proximity Group Overview
- Creating a Proximity Group
- Deleting a Proximity Group IP Address Block
- Deleting a Proximity Group

Proximity Group Overview

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

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

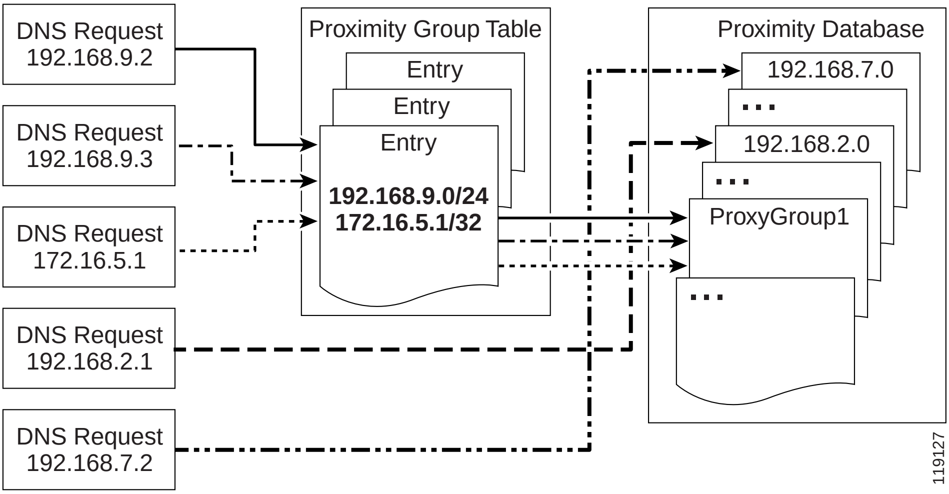
The benefits of proximity grouping include:

- Fewer probing activities performed by the GSS. The GSS probes the first requesting D-proxy from all configured zones to obtain the RTT value from each zone for the entire proximity group. This reduces the overhead associated with probing.
- Less space required for the PDB. Instead of multiple PDB entries, the GSS uses only one entry for multiple D-proxies.
- 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 illustrates how through proximity group entries 192.168.9.0/24 and 172.16.5.1/32, the DNS requests from D-proxies 192.168.9.2, 192.168.9.3, and 172.16.5.1 all map to the identified group name, *ProxyGroup1*. If no match is found in the PDB for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 9-3 Locating a Grouped Proximity Database Entry



Creating a Proximity Group

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

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

The syntax for this command is:

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

The options and variables are:

- *groupname*—Enter a unique alphanumeric name, with a maximum of 80 characters. Names that include spaces are not allowed.
- **ip** *ip-address*—The IP address block specified in dotted-decimal notation (for example, 192.168.9.0).
- **netmask** *netmas*k—The subnet mask of the IP address block specified in dotted-decimal notation (for example, 255.255.255.0).

This example shows how to create a proximity group called *ProxyGroup1* with an IP address block of 192.168.9.0 255.255.255.0:

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

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

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

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

Deleting a Proximity Group IP Address Block

To delete a previously configured IP address block from a proximity group, use the **no** form of the **proximity group** command. For example:

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

Deleting a Proximity Group

To delete a proximity group and all configured IP address blocks, use the **no** form of the **proximity group** command. For example:

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

Configuring Static Proximity Database Entries

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

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

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, follow these steps.

  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
  ```

  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.

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 and remain in the PDB until you delete them. In addition, static entries are not subject to the automatic database cleanup of least recently used entries when the PDB size is almost at the maximum number of entries. Use the **no proximity assign** command to delete static entries from the PDB.

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

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

To create static entries in the PDB, use the **proximity assign** global server load-balancing configuration mode command. The syntax for this command is:

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

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

The options and variable are:

- **group** *groupname*—Enter a unique alphanumeric name, 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*—The D-proxy IP address entry to be created in the PDB.
- **probe-target** *ip-address*—(Optional) An alternate IP address for the probing device to probe. Normally, the probing device transmits a probe to the requesting D-proxy IP address to calculate RTT. If you find that the D-proxy cannot be probed from the probing device, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.
- **zone-data** “*zoneId:RTT*”—(Optional) 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 (one day). To specify multiple static *zone:RTT* pairs in the proximity group, separate each entry within the quotation marks by a comma, but without spaces between the entries (for example, "3:450,22:3890,31:1000").

This example shows how to configure an alternative probing target for the proximity group *ISP1*:

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

This example shows how to configure an alternative probing target for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0):

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# proximity assign ip 192.168.8.0
probe-target 192.168.2.2
```

This example shows how to configure static RTT metrics for the proximity group ISP2 using zone indexes created previously through the primary GSSM:

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

This example shows how to configure static RTT metrics for D-proxy subnet 192.168.8.0 (assuming the global mask configuration is 255.255.255.0):

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

Deleting Static Entries from the Proximity Database

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

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

This example shows how to delete static RTT entries for the proximity group *ISP1*:

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

Deleting Entries from the Proximity Database

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

The syntax for this command is:

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

The options and variables are

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

Caution Use the **proximity database delete all** command only when you want to remove all entries from the PDB to have an empty database. Ensure that you want to permanently delete entries from the PDB before you enter this command. You cannot retrieve PDB entries once they are deleted.

- **assigned**—Removes all static entries from the PBD.
- **group** *name*—Removes all entries that belong to a named proximity group. Specify the exact name of a previously created proximity group.
- **inactive** *minutes*—Removes all dynamic entries that have been inactive for a specified time. Valid values are 0 to 43200 minutes.

- **ip** *ip-address* **netmask** *netmask*—Removes all proximity entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **no-rtt**—Removes all entries from the PDB that do not have valid RTT values.
- **probed**—Removes all dynamic entries from the PDB.

For example, to remove the D-proxy IP address 192.168.8.0 and subnet mask 255.255.255.0, enter:

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

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

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

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

If you attempt to overwrite an existing proximity database dump file with the same filename, the GSS displays the following message: `Proximity Database dump failed, a file with that name already exists.`

To dump entries contained in the PDB to a named file, use the **proximity database dump** command.

The syntax for this command is:

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

The options and variables are:

- *filename*—The name of the output file containing the PDB entries on the GSS disk. This file resides in the /home directory.
- **format**—Dumps the PDB entries in binary or XML format. Select binary encoding as the format type if you intend to load the contents of the file into the PDB of another GSS. The valid entries are:
  - **binary**—Dumps the assigned proximity entries in true binary format. This file can only be used with the **proximity database load** command
  - **xml**—Dumps the assigned proximity entries in XML format. The contents of an XML file includes the data fields along with the data descriptions. The contents of this file can be viewed using the **type** 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 two to four 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:
  - **all**—Dump static and dynamic entries from the PDB. This is the default.
  - **assigned**—Dump statically assigned proximity entries.
  - **probed**—Dump dynamically probed proximity entries.
- **entry-address** *ip-address*—The IP address of the PDB entry.
- **netmask** *netmask*—The subnet mask of the PDB entry in dotted-decimal notation (for example, 255.255.255.0).

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

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

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

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

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

Running a Periodic Proximity Database Backup

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

To force an immediate backup of the PDB residing in GSS memory, use the **proximity database periodic-backup now** command. The GSS sends the PDB entries to the system dump file as the proximity database file. Upon a reboot or restart, the GSS reads this file and loads the contents to initialize the PDB at boot time.

The syntax for this command is:

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 non-overlapping database entries.

To load a PDB from disk into GSS memory, use the **proximity database load** command. The syntax for this command is:

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

The options and variable are:

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

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

This example shows how to load the entries from the *GSS3PDB* file without overriding the existing entries in the GSS PDB:

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

For example, to override the same entries located in the existing GSS PDB, enter:

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

Initiating Probing for a D-proxy Address

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

There may be instances when you need to instruct the probing device in one or all zones (broadcast) to send a probe to a specific D-proxy address, obtain an RTT value, and save the entry in the PDB. To initiate direct probing to a specific D-proxy IP address or direct probing to one or more zones, use the **proximity probe** command.

The syntax for this command is:

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

The options and variables are:

- *dproxy_address*—The IP network address of the D-proxy that you want to probe from the probing device.
- **zone** *zoneId*—The ID of the proximity zone containing the probing device from which you want to initiate a probe. Available values are 1 to 32.
- **all**—The GSS instructs the probing devices in all configured zones to transmit a probe to the specified D-proxy IP address.

For example, to instruct the probing device in zone 1 to send a probe to the D-proxy at 172.16.5.7, enter:

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

Disabling Proximity Locally on a GSS for Troubleshooting

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

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

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

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

This example shows how to locally disable proximity on a GSS device using the **proximity stop** command:

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

This example shows how to locally reenable proximity on a GSS device, using the **proximity start** command:

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