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:

Each GSS supports a comprehensive set of **show** CLI commands to display network proximity statistics for the device. In addition, the primary GSSM GUI displays statistics about proximity operation for the GSS network. Refer to Chapter 10, Monitoring GSS Global Server Load-Balancing Operation for details about viewing network proximity statistics.

Network Proximity Overview

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

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

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

This section describes the major functions in GSS network proximity:

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

Proximity Zones

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

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

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

Probe Management and Probing

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

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

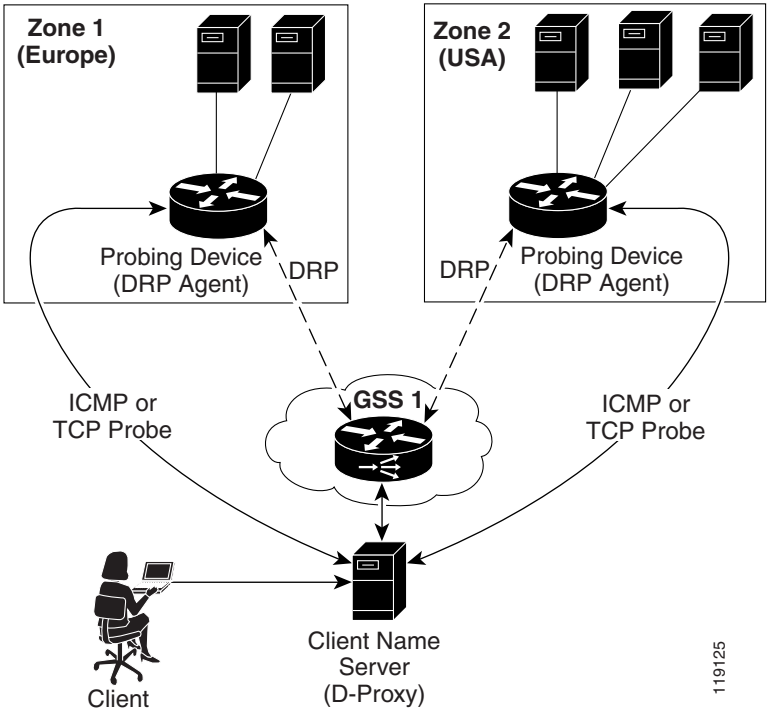
Each DRP agent accepts probing instructions from the GSS and returns probing results to the GSS based on the DRP protocol. DRP allows for the authentication of packets exchanged between the DRP agent and the GSS.

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

The primary GSSM supports the creation of proximity groups which allow you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its PDB as a single entry. Instead of multiple PDB entries, the GSS uses only one entry in the PDB for multiple D-proxies. The GSS treats all D-proxies in a proximity group as a single D-proxy when responding to DNS requests with the most proximate answers. Requests from D-proxies within the same proximity group receive the RTT values from the database entry for the group. The benefits of proximity grouping include less probing activities performed by the GSS, less space required for the PDB, and user flexibility in assigning alternative probing targets or static proximity metrics to a group.

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

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

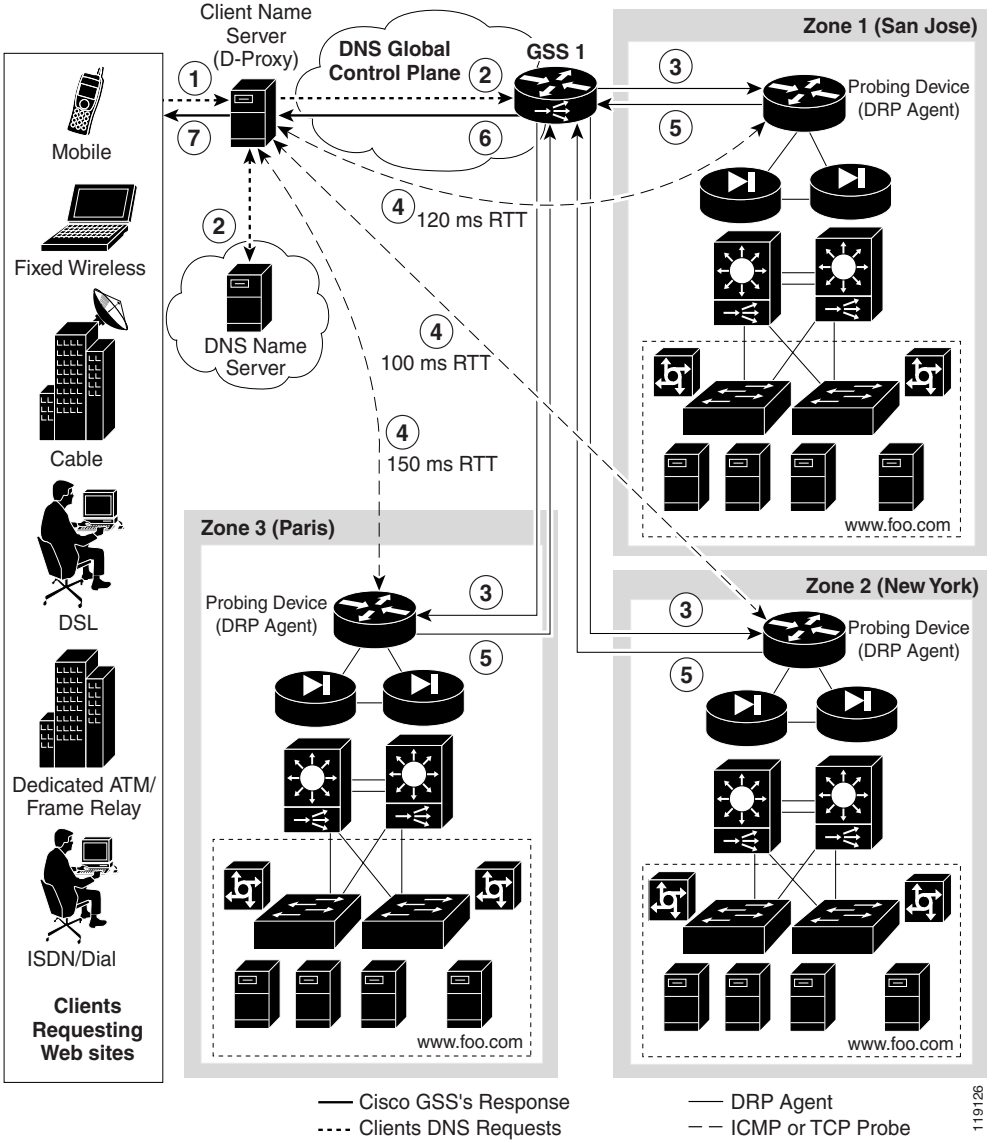
When the PDB reaches a maximum of 500,000 entries, the GSS does not add entries to the PDB and any new requests for answers result in a failure. The GSS tracks how many entries are dropped because the maximum limit has been reached. Once the number of PDB entries drops below 500,000, the GSS resumes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

Example of Network Proximity

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

1. A client performs an HTTP request for *www.foo.com*. The content for this website is supported at three different data centers.
2. The DNS global control plane infrastructure processes this request and directs the client D-proxy to GSS 1. The GSS offloads the site selection process from the DNS global control plane. The client's local D-proxy queries GSS1 for the IP address associated with www.foo.com. The GSS accepts the DNS query.
3. If the request matches a proximity DNS rule configured on the GSS, the GSS performs an internal PDB lookup. If the lookup fails, the GSS sends DRP queries to the DRP agent configured for each zone.
4. When the DRP agent in each zone receives a DRP request, they measure RTT from their associated zone back to the requesting client D-proxy device, using either ICMP 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 are allowed within each GSS proximity environment. You can change zone configuration at any time by deleting or adding a zone, or by moving a zone from one location to another location.
- For each zone, identify the probing device and, optionally, the backup probing device. Each probing device represents the topological location of its associated zone and also reflects the zone's expected network behavior in terms of connectivity to the internet. The probing device is the DRP agent located within the zone.
- Each GSS network can contain a maximum of eight GSS devices. GSS devices can be added and deleted anytime. The GSS does not have to reside within a zone.
- To use proximity, you must:
  - Associate a proximity zone with a location
  - Assign a location that is associated with a proximity zone to an answer

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

Network Proximity Quick Start Guide

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

Table 9-1 Proximity Configuration Quick Start

Task and Command Example

1. Log in to the CLI of each GSS in the network, enable privileged EXEC mode, and synchronize its system clock with an NTP server.
 	
For example:
 	
`gss1.example.com> enable`
`gss1.example.com# config`
`gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3`
`gss1.example.com(config)# ntp enable`

2. Configure a Cisco router as a DRP agent in one or more proximity zones.
3. Log in to the primary GSSM GUI.
4. Click the **Traffic Mgmt** tab, then click the **Zone** navigation link to access the Zones details page. Create one or more proximity zones in the Zones details page by specifying the index for the proximity zone, the IP address of the primary probe device, and the IP address of the backup probe device.
5. Click the **Proximity** navigation link to access the Proximity details page (Traffic Mgmt tab). At the State option, click the **Enabled** option button to globally enable proximity across the entire proximity network.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
6. If you need to modify one or more of the global proximity configuration default settings in the Proximity details page, perform the following: • In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses. Use this parameter as an attempt to increase the number of D-proxies supported in the PDB. You can enter the mask in either dotted-decimal notation or as a prefix length in CIDR bit count notation. • In the Entry Inactivity Timeout field, enter the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes the entry from the PDB. • In the Equivalence Window field, enter a percentage value that the GSS applies to the most proximate RTT value to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Use this parameter to adjust the granularity of the proximity decision process. • In the Refresh Probe Interval field, enter the frequency of the refresh probing process to probe and update RTT values in the PDB. • In the Initial Probe Method drop-down list, specify the type of probe method (TCP or ICMP) used initially by the Cisco IOS-based router during the probe discovery process of the requesting client's D-proxy. • In the Acceptable RTT field, enter a value that the GSS uses as an largest acceptable RTT value when determining the most proximate answer. Use this parameter to adjust the granularity of the proximity decision process. • In the Acceptable Zone field, enter the minimum percentage of zones that the GSS requires to return RTT values before it returns a proximity answer. Use this parameter to adjust the granularity of the proximity decision process. • In the Wait drop-down list, enable or disable the proximity wait state. • In the DRP Authentication drop-down list, enable or disable DRP authentication.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
7. If you enabled DRP Authentication and no DRP keys exist for the GSS, click the **Add Proximity Key** navigation link from the Proximity details page. Create one or more DRP keys in the Creating New DRP Key details page. Each DRP key includes a key identification number and a key authentication string. Click the **Add** button to save each DRP key.
8. Click the **Submit** button to save your global proximity configuration changes.
9. Associate a location to a proximity zone. Use either the Creating New Location details page for a new location or the Modifying Location details page for an existing location. Repeat this step if you have multiple locations that you wish to assign to a proximity zone.
10. Assign a location that is associated with a proximity zone to an answer. Use either the Creating New Answer details page for a new answer or the Modifying Answer details page for an existing answer. Repeat this step if you have multiple answers that you want to assign to an associated proximity location.
11. Access the DNS Rules Builder as follows: **a.** Click the **DNS Rules** tab. **b.** Click the **DNS Rules** navigation link. The DNS Rules list appears. **c.** Click either the **Open Rule Builder** icon (if this is a new DNS rule) or the **Modify DNS Rule Using Rule Builder Interface** icon (if this is an existing DNS rule) to access the DNS Rule Builder. **Note** You can configure the network proximity global server load-balancing application only from the DNS Rule Builder, not from the DNS Rule Wizard. Use the DNS Rule Builder to enable proximity in a DNS rule.

Table 9-1 Proximity Configuration Quick Start (continued)

Task and Command Example
12. Enable network proximity in a DNS rule using the DNS Rule Builder. Define the following DNS rule configuration information: **a.** For each balance clause that is to perform proximity, click the **Proximity Enable** checkbox. **b.** To change the proximity acceptable RTT for the balance clause to a different value from the global proximity configuration, enter a value in the RTT field. **c.** To change the proximity acceptable zone for the balance clause to a different value from the global proximity configuration, enter a value in the Zone field. **d.** To change the proximity wait state to a different setting than the global proximity configuration, make a selection from the Wait drop-down list.
13. Log on to the CLI of a GSS in the network and enable privileged EXEC mode. `gssm1.example.com> enable`

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

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

Configuring a Cisco Router as a DRP Agent

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

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

Choosing a Cisco Router as a DRP Agent

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

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

Configuring the DRP Agent

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

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

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

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

Cisco IOS Release 12.1 Interoperability Considerations

If you use a GSS in a network proximity zone configuration with a Cisco router running IOS release 12.1, it is important to ensure the DRP authentication configuration is identical on both devices. For example, if you intend to perform DRP authentication between a GSS and a Cisco IOS 12.1 router, ensure that you properly enable and configure authentication on both devices. The same is true if you choose not to use DRP authentication; you disable authentication on both devices.In the case that you disable DRP authentication on a Cisco IOS 12.1 router but enable DRP authentication on a GSS, all measurement probes sent by a GSS to the Cisco IOS-based router will fail. This condition occurs because the Cisco IOS 12.1 router fails to recognize the DRP echo query packets sent by a GSS and the GSS cannot detect a potential failure of measurement packets sent to the router. In this case, the GSS identifies the Cisco IOS-based router as being ONLINE in its **show statistics proximity probes detailed** CLI command, yet the measurement response packets monitored in the Measure Rx field do not increment. Together, these two conditions may indicate a DRP authentication mismatch.

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

- To verify the DRP authentication configuration on the Cisco router running IOS release 12.1, enter the **show ip drp** command. If the line `Authentication is enabled, using "test" key-chain` appears in the output (where `"test"` is the name of your key-chain), DRP authentication is configured on the router. If this line does not appear in the output, DRP authentication is not configured.
- To verify the DRP authentication configuration on the primary GSSM GUI, access the Global Proximity Configuration details page (Traffic Mgmt tab) and observe if the DRP Authentication selection is set to Enabled or Disabled (see the "Configuring Proximity" section for details).

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

Synchronizing the GSS System Clock with an NTP Server

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

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

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

Note For details on logging in to a GSS device and enabling privileged EXEC mode at the CLI, refer to the "Logging in to the CLI and Enabling Privileged EXEC Mode" section.

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

ntp-server *ip_or_host*

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

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

ntp enable

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

```
gss1.example.com> enable
gss1.example.com# config
gss1.example.com(config)# ntp-server 172.16.1.2 172.16.1.3
gss1.example.com(config)# ntp enable
```

Creating Zones Using the Primary GSSM GUI

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

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

This section includes the following procedures:

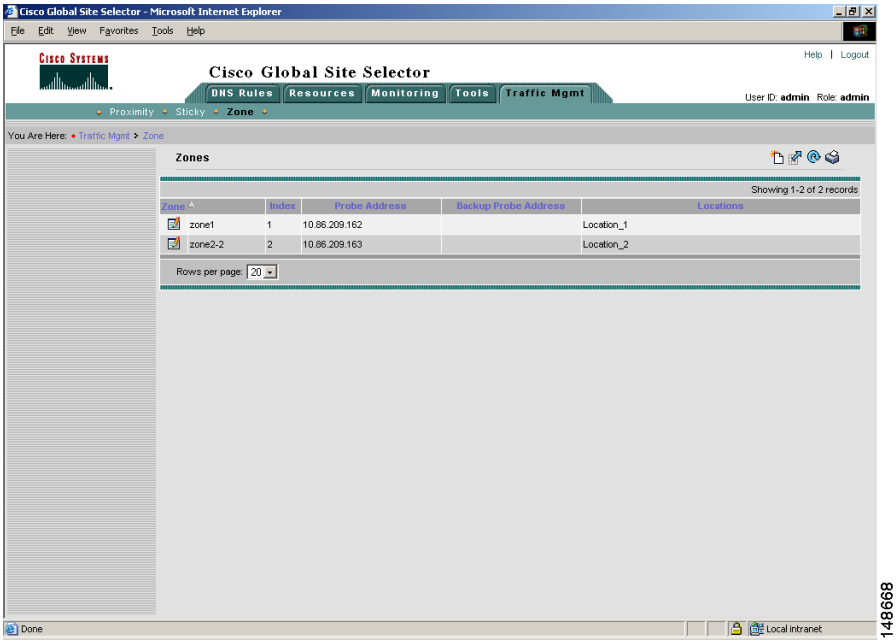
- Creating a New Proximity Zone
- Modifying a Proximity Zone
- Deleting a Proximity Zone
- Associating a Proximity Zone With a Location
- Associating a Proximity-Based Location with an Answer

Creating a New Proximity Zone

To create a proximity zone from the primary GSSM GUI:

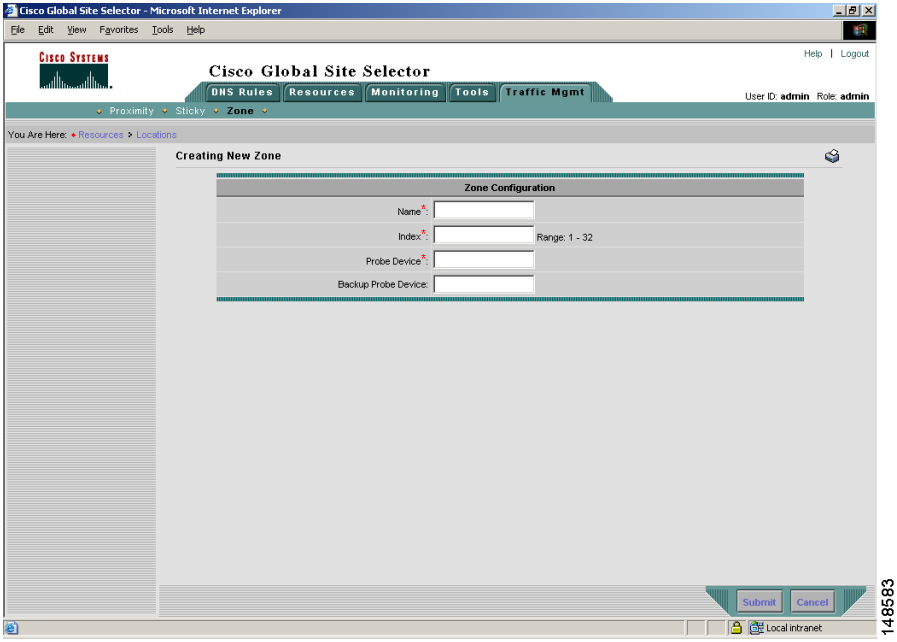
1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zone** navigation link. The Zones list page appears (Figure 9-3).

Figure 9-3 Zones List Page



3. Click the **Create Zone** icon. The Creating New Zone detail page appears (Figure 9-4).

Figure 9-4 Creating New Zone Detail Page



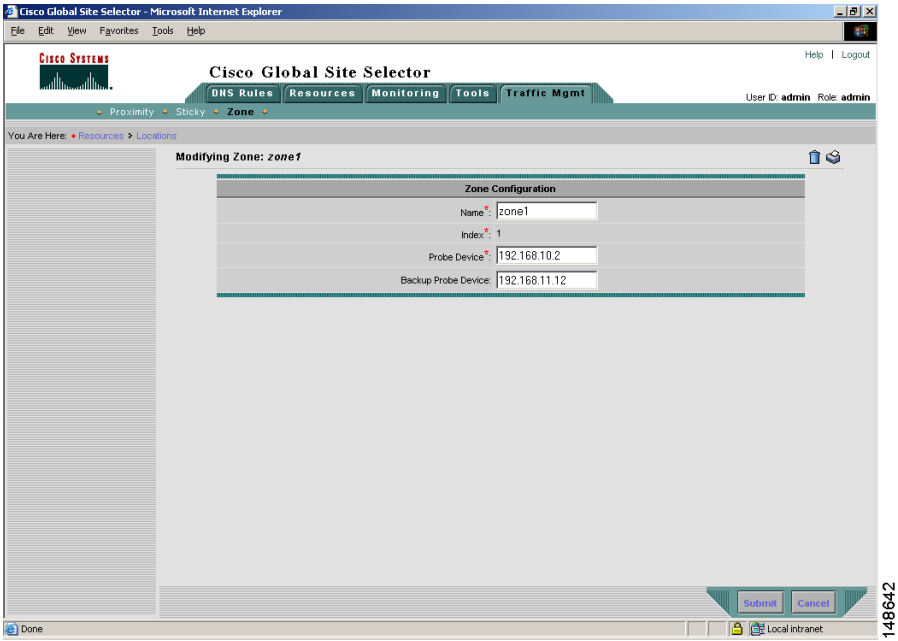
4. In the Name field, enter an alphanumeric description of the zone. Only alphanumeric characters and the underscore ("_") character are allowed.
5. In the Index field, specify the numerical identifier of the proximity zone. Enter an integer from 1 to 32. There is no default.
6. In the Probe Device field, enter the IP address of the primary probe device servicing this zone.
7. In the Backup Probe Device field, enter the IP address of the backup probe device for this zone.
8. Click the **Submit** button to save your zone. You return to the Zones list page.

Modifying a Proximity Zone

To modify a proximity zone from the primary GSSM GUI:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zone** navigation link. The Zones list page appears.
3. Click the **Modify Zone** icon located to the left of the zone you want to modify. The Modifying Zone details page appears (Figure 9-5).

Figure 9-5 Modifying Zone Details Page



4. Use the fields provided to modify the zone configuration.

Note The zone Index value cannot be modified. To change the zone index, delete the zone (see the "Deleting a Proximity Zone" section) and create a new zone containing a different index.

5. Click **Submit** to save your configuration changes and return to the Zones list page.

Deleting a Proximity Zone

To delete a proximity zone from the primary GSSM GUI:

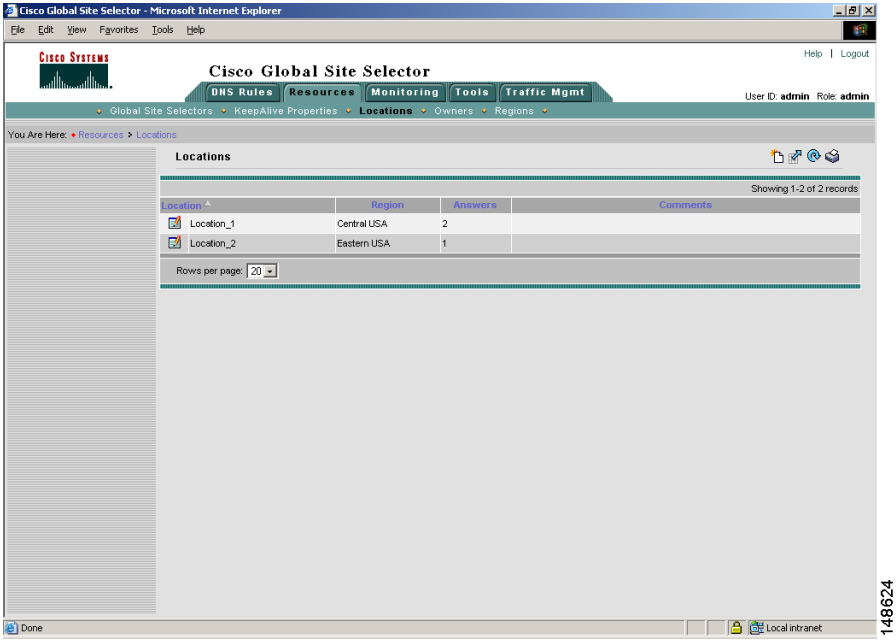
1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Zones** navigation link. The Zones list page appears.
3. Click the **Modify Zone** icon located to the left of the zone that you want to delete. The Modifying Zone details page appears (see Figure 9-5).
4. Click the **Delete Zone** icon in the upper right corner of the page. The GSS software prompts you to confirm your decision to delete the zone.
5. Click **OK** to confirm your decision and return to the Zones list page.

Associating a Proximity Zone With a Location

To associate a proximity zone with a location:

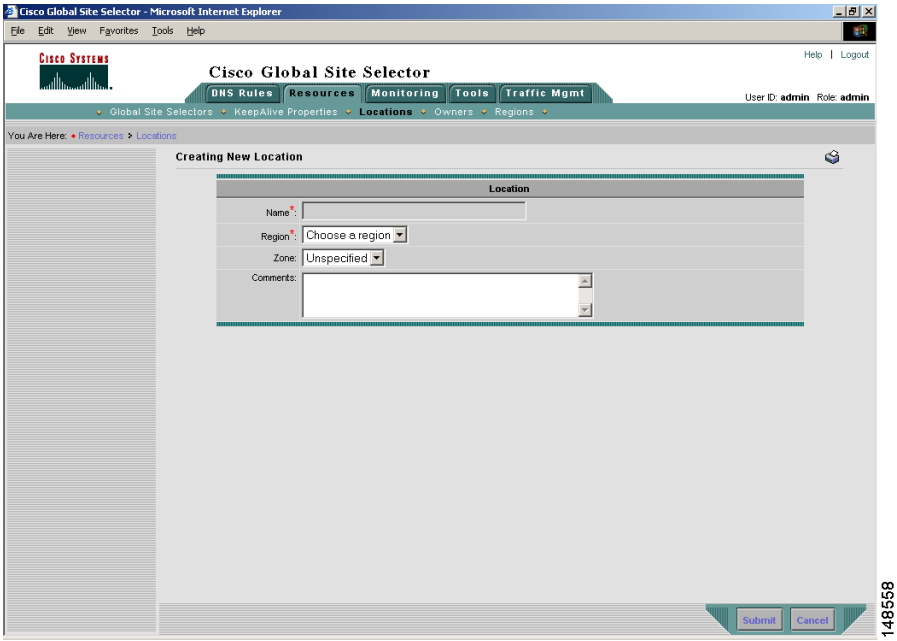
1. From the primary GSSM GUI, click the **Resources** tab.
2. Click the **Locations** navigation link. The Locations list page appears (Figure 9-6).

Figure 9-6 Locations List Page



3. Click either the **Create Location** icon (if this is a new location) or the **Modify Location** icon (if you are adding the proximity zone to an existing location). The Location details page appears (Figure 9-7). For details about creating a location, refer to Chapter 2, Configuring Resources.

Figure 9-7 Creating New Location Details Page



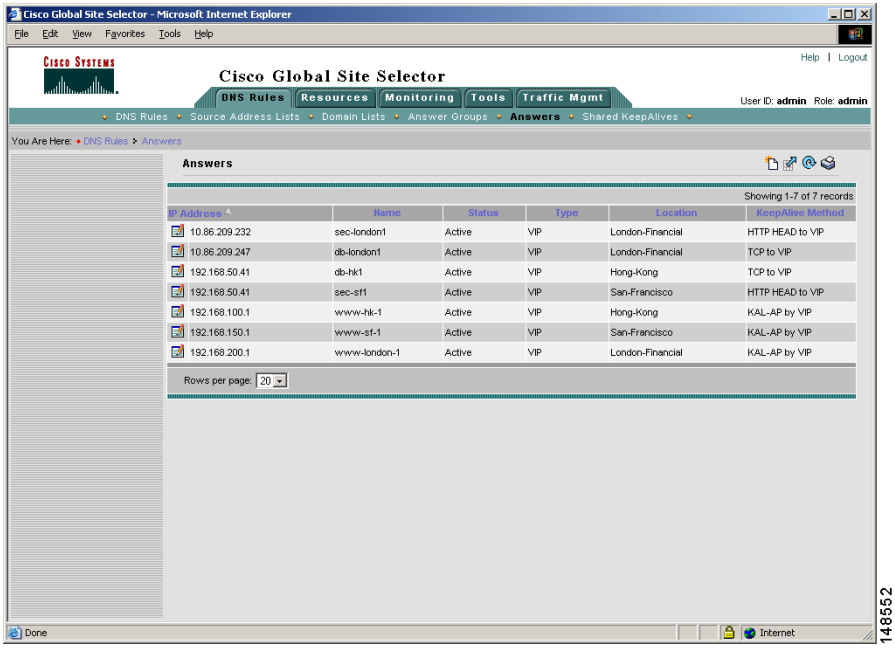
4. Click the **Zone** drop-down list and associate a zone with the location. There should be a logical connection between the zone and the location.
5. Click **Submit** to save changes to your location and return to the Locations list page.

Associating a Proximity-Based Location with an Answer

To assign a location that is associated with a proximity zone to an answer:

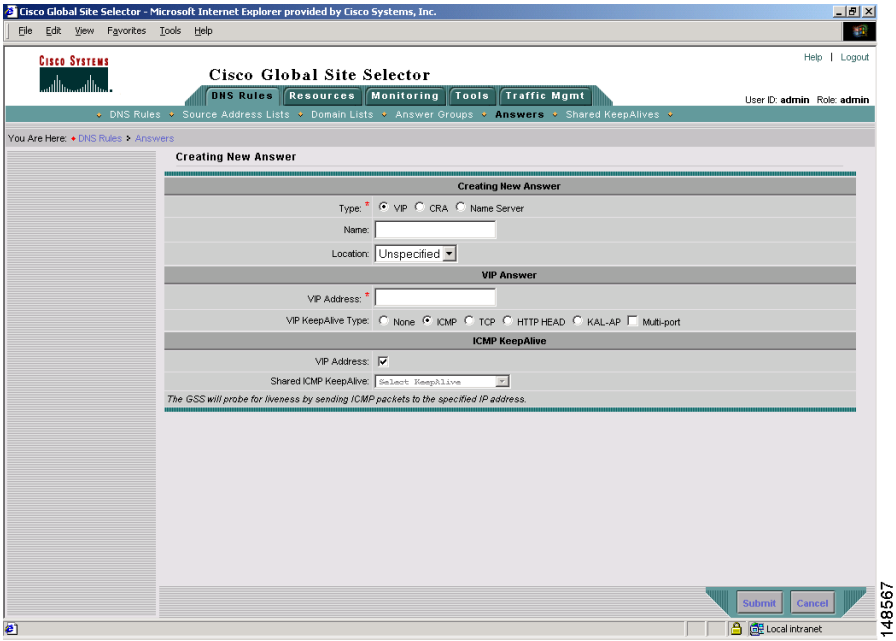
1. From the primary GSSM GUI, click the **DNS Rule** tab.
2. Click the **Answers** navigation link. The Answers list page appears (Figure 9-8).

Figure 9-8 Answers List Page



3. Click either the **Create Answer** icon (if this is a new answer) or the **Modify Answer** icon (if you are adding the location to an existing answer). The Answer details page appears (Figure 9-9).

Figure 9-9 Creating New Answer Details Page



4. In the Type field, click the **VIP** option button. The VIP Answer section appears in the details page.
5. In the Name field, enter a name for the VIP-type answer that you are creating. Specifying a name for an answer is optional.
6. From the Location drop-down list, select an appropriate GSS location that is associated with a proximity zone.
7. Complete the remaining VIP-type answer parameters as described in Chapter 6, Configuring Answers and Answer Groups.
8. Click **Submit** to save changes to your location and return to the Answers list page.
9. Repeat this procedure if you have multiple answers that you want to assign to an associated proximity location.

Configuring Proximity Using the Primary GSSM GUI

This section discusses how to configure the GSS for network proximity operation from the primary GSSM GUI and how to add proximity to a DNS rule in the DNS Rule Builder. It includes the following procedures:

- Configuring Proximity
- Creating DRP Keys
- Deleting DRP Keys
- Using the DNS Rule Builder to Add Proximity to a DNS Rule

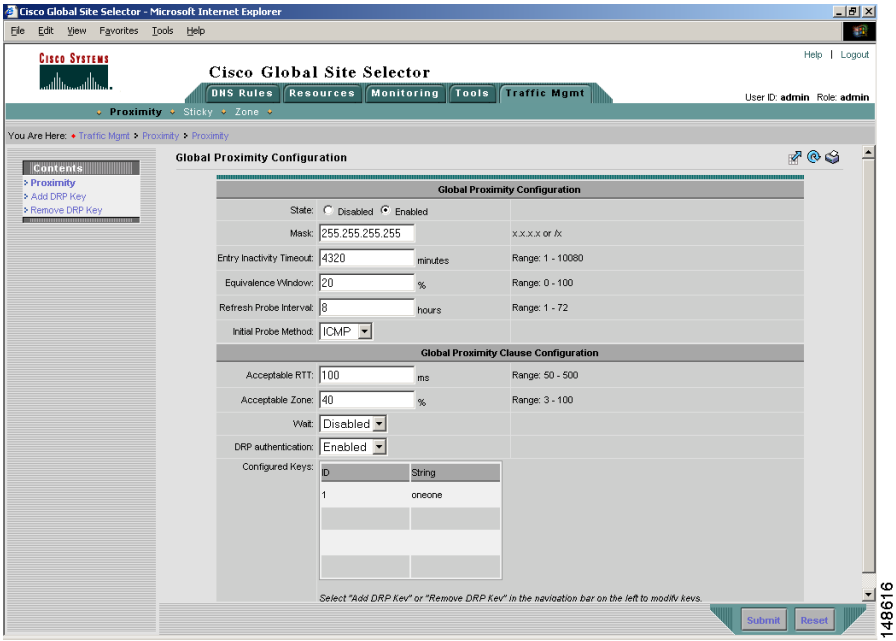
Configuring Proximity

The GSS includes a set of proximity settings that function as the default values used by the GSS network when you enable proximity in a DNS rule. You enable proximity and modify the global proximity setting for the GSS network using the fields on the Global Proximity Configuration details page of the Traffic Mgmt tab. Changing a global proximity setting and applying that change is immediate and modifies the default values of the proximity settings used by the DNS Rule Builder.

To configure proximity from the primary GSSM GUI:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (Figure 9-10).

Figure 9-10 Global Proximity Configuration Details Page



3. At the State option, click the **Enabled** option button to globally enable proximity across the entire GSS network. To globally disable proximity across the GSS network, click the **Disabled** option button.
4. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses as an attempt to increase the number of supported D-proxies in the PDB. Enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit count notation (for example, /24). The default global mask is 255.255.255.255.

   When you define a proximity group for incoming D-proxy addresses (see the "Creating Proximity Groups" section), if the incoming D-proxy address does not match any of the entries in a defined proximity group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

5. In the Entry Inactivity Timeout field, enter the maximum time interval that can pass without the PDB receiving a lookup request for an entry before the GSS removes that entry. This value defines the PDB entry age-out process. Once an entry reaches the inactivity time, the GSS removes the selected dynamic entries from the PDB. Enter a value from 1 to 10080 minutes (168 hours). The default value is 4320 minutes (72 hours).
6. In the Equivalence Window field, enter a percentage value that the GSS applies to the most proximate RTT value (the closest) to help identify the relative RTT values of other zones that the GSS should consider as equally proximate. Through the Equivalence Window percentage, you define an RTT window that the GSS uses to consider zones equal. The Equivalence Window value enables the GSS to prioritize between multiple distributed servers that have similar server-to-client RTT values. The GSS considers any RTT value that is less than or equal to the lowest RTT plus the percentage to be equivalent to the lowest RTT value. The GSS chooses one answer from a set of answers in equal zones.

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

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

   The GSS determines that Zone1 has the lowest RTT value. In this case, the GSS adds 20 percent (20 ms) to the RTT value to make Zone 1 and 2 equally proximate in regards to the GSS selecting an answer. The RTT equivalence window range is from 100 ms to 120 ms, and the GSS considers any zone that returns an RTT value in that range to be equally proximate.

   Use this parameter to adjust the granularity of the proximity decision process. Enter an equivalence window value from 0 to 100 percent. The default value is 20 percent.
7. In the Refresh Probe Interval field, enter the frequency of the refresh probing process to probe and update RTT values for the entries in the PDB. Enter a value from 1 to 72 hours. The default value is 8 hours.

8. In the Initial Probe Method drop-down list, specify the type of probe method used initially by the Cisco IOS-based router during the probe discovery process with the requesting client's D-proxy. If the Cisco router attempts the specified probe method and the D-proxy does not recognize the method, the GSS automatically chooses a different probe method to contact the D-proxy. The available choices for the initial probe method are ICMP 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.
9. In the Acceptable RTT field, enter a value that the GSS uses as an acceptable RTT value when determining the most proximate answer. If the zones configured on the GSS report an RTT that is less than the specified Acceptable RTT value, the GSS does the following:
   a. Disregards the acceptable percentage of zones.
   b. Considers that there is sufficient proximity data to make a proximity decision.
   c. Uses the zones reporting less than or equal to this value in the proximity decision.

   Use this parameter to adjust the granularity of the proximity decision process. Enter an acceptable RTT value from 50 to 500 ms. The default value is 100 ms.

10. In the Acceptable Zone field, enter a percentage value that the GSS uses to determine if an acceptable number of zones return valid RTT values. The Acceptable Zone value specifies the percentage of all zones configured and used for a DNS rule and answer group. If an insufficient number of zones report RTT information, the balance clause fails and the GSS processes a new clause. For example, if the answer group associated with a clause includes answers that correspond to five different zones and you specify an Acceptable Zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of two zones to satisfy the 40 percent criteria. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

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

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

11. In the Wait drop-down list, enter the GSS proximity wait-state condition:
    - **Enabled**—The GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. The GSS does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process.
    - **Disabled**—The GSS does not wait to perform a proximity selection if it has not received the appropriate RTT and zone information based on other proximity settings. In this case, the GSS proceeds to the next balance clause in the DNS rule.

    The default setting is Disabled.

12. In the DRP Authentication drop-down list, enter the DRP authentication state:
    - **Enabled**—The GSS authenticates packets that it exchanges with the DRP agent in a probing device through the exchange of DRP keys. The key authenticates the DRP requests and responses sent between the GSS and the DRP agent. You enable DRP authentication by creating a DRP key (see the "Creating DRP Keys" section).
    - **Disabled**—The GSS does not perform DRP authentication with the DRP agent.

    The default setting is Disabled.
13. Click the **Submit** button to save your global proximity configuration changes.

Creating DRP Keys

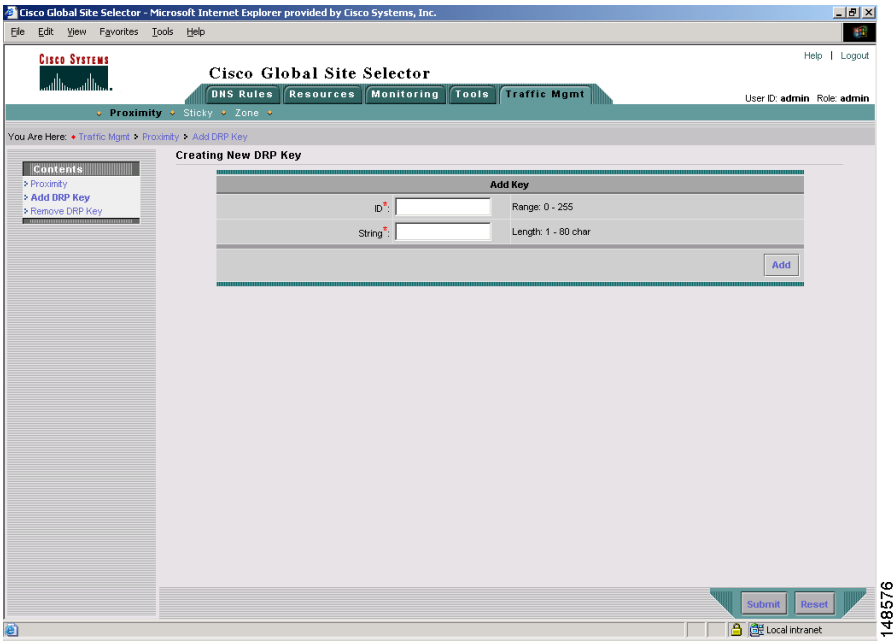
DRP supports the authentication of packets exchanged between the DRP agent (probing device) and the DRP client (the GSS). To enable DRP authentication for network proximity, create one or more DRP keys. Each DRP key contains a key identification number and a key authentication string. The primary GSSM GUI supports a maximum of 32 keys.

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

To create a DRP authentication key:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (see Figure 9-10).
3. Click the **Add DRP Key** navigation link. The Creating New DRP Key details page appears (Figure 9-11).

Figure 9-11 Creating New DRP Key Details Page



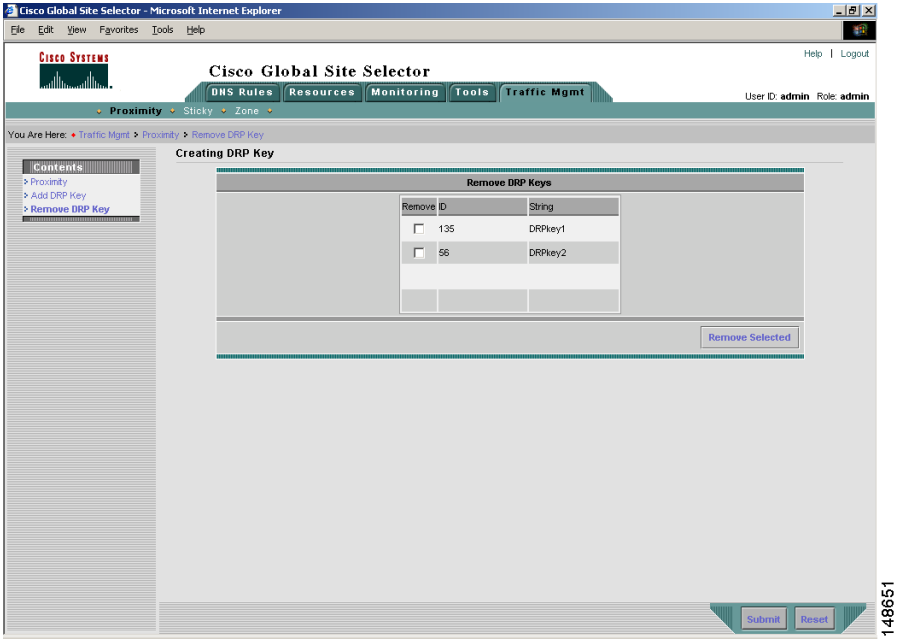
4. Enter the following values to create a DRP key:
   - **ID**—The identification number of a secret key used for encryption. The GSS uses the ID value to retrieve the key string that is used to verify the DRP authentication field. The ID value must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The range of key identification numbers is from 0 to 255.
   - **String**—The authentication string that is sent and received in the DRP packets. The string must be the same between the DRP agent on the Cisco IOS-based router and the GSS. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.
5. Click the **Add** button to create your DRP authentication key.
6. Click the **Submit** button to save your global proximity configuration changes.
7. Repeat this procedure to create additional DRP keys. The primary GSSM supports a maximum of 32 keys.

Deleting DRP Keys

To remove DRP authentication keys:

1. From the primary GSSM GUI, click the **Traffic Mgmt** tab.
2. Click the **Proximity** navigation link. The Global Proximity Configuration details page appears (see Figure 9-10).
3. Click the **Remove DRP Key** navigation link. The Remove DRP Key details page appears (Figure 9-12).

Figure 9-12 Remove DRP Key Details Page



4. Click the check box accompanying each DRP key that you want to remove from the list, then click the **Remove Selected** button. The GSS removes the selected DRP keys from the page.

Using the DNS Rule Builder to Add Proximity to a DNS Rule

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

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

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

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

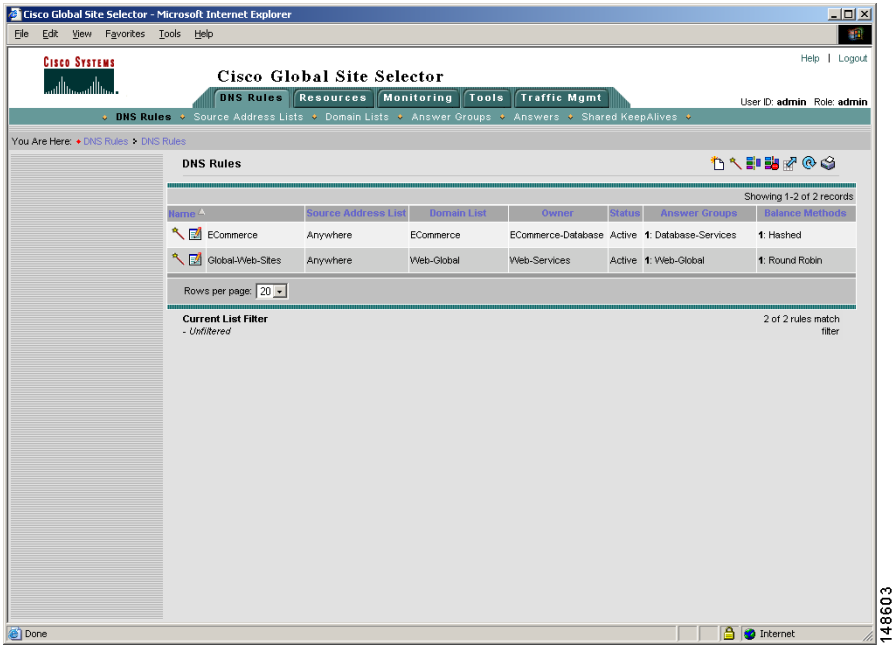
When there are no valid answers in the answer group of a proximity balance clause, the GSS skips that balance clause and moves on to the next clause listed in the DNS rule unless you specify a proximity Wait condition. In that case, the GSS waits to perform a proximity selection until it receives the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

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

To use the DNS Rule Builder to add proximity balance clauses to a DNS rule:

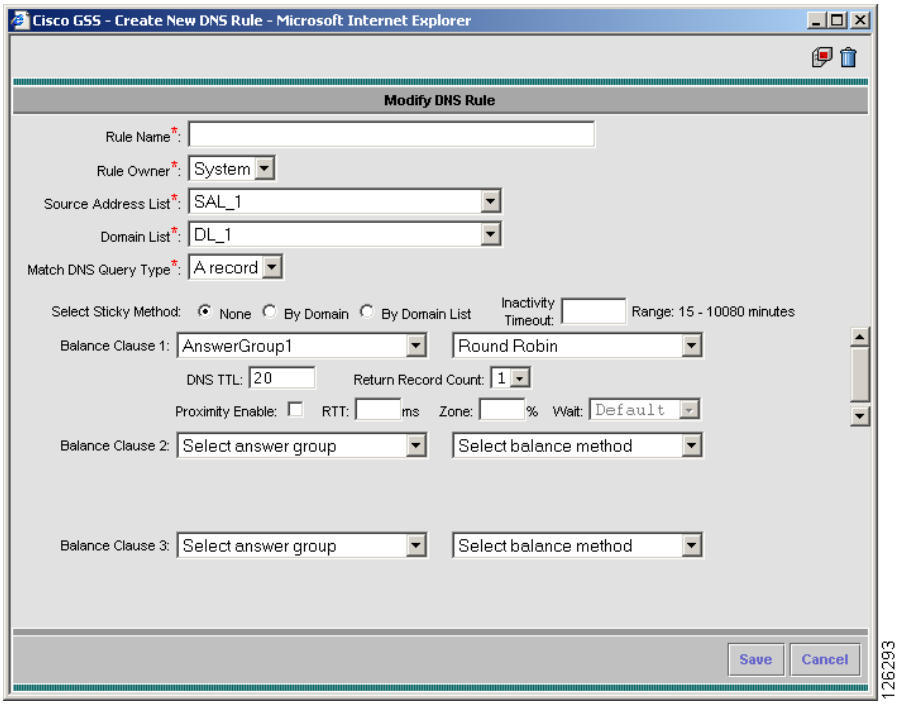
1. From the primary GSSM GUI, click the **DNS Rules** tab, then click the **DNS Rules** navigation link. The DNS Rules list page appears (Figure 9-13).

Figure 9-13 DNS Rules List Page



2. Click the **Open Rule Builder** icon. The Create New DNS Rule page opens in a separate window (Figure 9-14).

Figure 9-14 Create New DNS Rule Window



3. Develop your DNS rule as outlined in steps 3 through 8 in the "Building DNS Rules Using the DNS Rule Builder" section of Chapter 7, Building and Modifying DNS Rules.

4. At the Balance Clause 1 heading:
   - Select the answer group component of your first answer group and balance method pairing from the drop-down list. This is the first effort performed by the GSS to select the most proximate answer for the DNS query. Ensure that the answers in the answer group are contained in locations that are tied to a zone.
   - Select the balance method for the answer group from the drop-down list.
5. Specify the following proximity parameters as part of the DNS rule balance clause:
   - **Proximity Enable**—To activate network proximity for the balance clause, click the Proximity Enable checkbox. This checkbox appears only when the answers in the answer group are contained in locations that are tied to a zone.
   - **RTT**—To change the proximity-acceptable RTT for the balance clause to a different value from the global proximity configuration, enter a value in the RTT field. The GSS uses this value as the user-specified acceptable RTT when determining the most proximate answer. If the zones configured on the GSS report an RTT that is less than the specified Acceptable RTT value, the GSS does one of the following:
     - Disregards the acceptable percentage of zones.
     - Considers that there is sufficient proximity data to make a proximity decision.
     - Uses the zones reporting less than or equal to this value in a proximity decision.

     Enter an acceptable RTT value from 50 to 500 ms. The default value is 100 ms.

- **Zone**—To change the proximity-acceptable zone percentage for the balance clause to a different value from the global proximity configuration, enter a value in the Zone field. The Acceptable Zone value specifies the percentage of all zones configured and used for a DNS rule and answer group. If an insufficient number of zones report RTT information, the balance clause fails and the GSS processes a new clause. For example, if the answer group associated with a clause includes answers that correspond to five different zones and you specify an Acceptable Zone setting of 40 percent, the GSS must receive valid RTT values from a minimum of two zones to satisfy the 40 percent criterion. If the GSS does not receive valid RTT values from at least two zones, it determines that the balance clause has failed.

  Enter a percentage of zones from 3 to 100 percent. The default value is 40 percent.

- **Wait—**To change the proximity wait state to a different setting than the global proximity configuration, make a selection from the drop-down list. Enter the GSS proximity wait state condition:
  - **Default**—Always use the globally defined proximity wait state.
  - **Enabled**—The GSS will wait to perform a proximity selection until it receives the appropriate RTT and zone information based on the proximity settings. While the GSS waits for sufficient proximity data, it does not return an answer to the requesting client's D-proxy until the GSS obtains sufficient proximity data to complete the selection process.
  - **Disabled**—The GSS does not wait to perform a proximity selection if it has not received the appropriate RTT and zone information based on other proximity settings. In this case, the GSS proceeds to the next balance clause in the DNS rule.

6. Repeat steps 4 and 5 to select additional answer group and balance method pairings for Balance Clause 2 and Balance Clause 3.
7. Click **Save** to save your DNS rule and return to the DNS Rules list page. The DNS rule is now active and processing incoming DNS requests.

Configuring Proximity Using the GSS CLI

This section describes how to configure a GSS device for network proximity operation from the CLI. From the primary GSSM CLI, you can create proximity groups to obtain better scalability of your GSS proximity configuration and to allow for ease of proximity group creation through automation scripts. You can also use the CLI of each GSS in your proximity network to perform PDB activities on an individual GSS basis, such as configuring static proximity entries, removing PDB entries from GSS memory, dumping entries from the PDB to a named file, forcing an immediate backup of the PDB, or loading and merging PDB from a file.

The section includes the following procedures:

Logging in to the CLI and Enabling Privileged EXEC Mode

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

To log in to a GSS device and enable privileged EXEC mode at the CLI:

1. Power on your GSS. After the GSS boot process completes, the software prompts you to log in to the device.
2. If you are remotely logging in to the GSS device (Global Site Selector or Global Site Selector Manager) through Telnet or SSH, enter the host name or IP address of the GSS to access the CLI.

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

For details about making a direct connection to the GSS device using a dedicated terminal and about establishing a remote connection using SSH or Telnet, refer to the *Cisco Global Site Selector Getting Started Guide*.

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

```
gss1.example.com>
```

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

```
gss1.example.com> enable
gss1.example.com#
```

Creating Proximity Groups

This section includes the following topics:

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

Proximity Group Overview

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

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

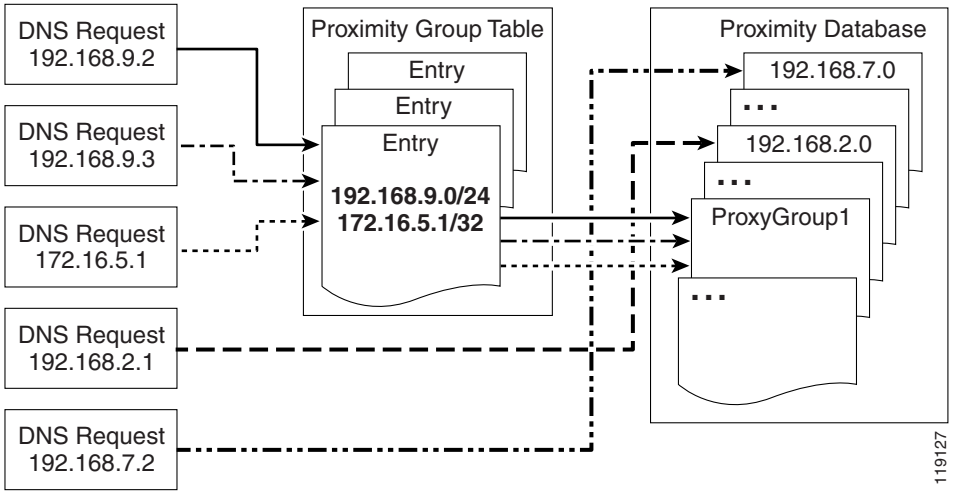
The benefits of proximity grouping include the following:

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

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

Figure 9-15 illustrates how through proximity group entries 192.168.9.0/24 and 172.16.5.1/32, the DNS requests from D-proxies 192.168.9.2, 192.168.9.3, and 172.16.5.1 all map to the identified group name, *ProxyGroup1*. If no match is found in the PDB for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 9-15 Locating a Grouped Proximity Database Entry



Creating a Proximity Group

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

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

The syntax for this command is:

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

The options and variables are:

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

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

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

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

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

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

Deleting a Proximity Group IP Address Block

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

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

Deleting a Proximity Group

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

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

Configuring Static Proximity Database Entries

This section describes how to configure static entries in the PDB. It includes the following procedures:

- Adding Static Proximity Entries
- Deleting Static Entries from the Proximity Database

Adding Static Proximity Entries

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

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

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

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

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

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

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

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

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

The options and variable are:

- **group** *groupname*—Enter a unique alphanumeric name for a group of static entries, with a maximum of 16 characters. Use only alphanumeric characters and the underscore ("_") character. Each static proximity group must have a unique name.
- **ip** *entryaddress*—The D-proxy IP address entry to be created in the PDB.
- **probe-target** *ip-address*—(Optional) An alternate IP address to probe by the probing device. Normally, the probing device transmits a probe to the requesting D-proxy IP address to calculate RTT. If you find that the D-proxy cannot be probed from the probing device, you can identify the IP address of another device that can be probed to obtain equivalent RTT data.
- **zone-data** "*zoneId:RTT*"—(Optional) The calculated RTT value for a zone, specified in "*zoneId:RTT*" format. For example, enter `"1:100"` to specify zone 3 with an RTT of 100 seconds. Valid entries for *zoneID* are from 1 to 32, and must match the proximity zone index specified through the primary GSSM GUI (see the "Synchronizing the GSS System Clock with an NTP Server" section). Valid entries for the *RTT* value are from 0 to 86400 seconds (one day). To specify multiple static *zone:RTT* pairs in the proximity group, separate each entry within the quotation marks by a comma, but without spaces between the entries (for example, "3:450,22:3890,31:1000").

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

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

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

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

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

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

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

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

Deleting Static Entries from the Proximity Database

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

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

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

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

Deleting Entries from the Proximity Database

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

The syntax for this command is:

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

The options and variables are

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

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

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

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

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

```
gss1.example.com# proximity database delete ip 192.168.8.0
255.255.255.0
```

Dumping Proximity Database Entries to a File

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

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

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

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

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

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

The syntax for this command is:

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

The options and variables are:

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

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

- **entry-type**—Specifies the type of PDB entries to output: static, dynamic, or both. The valid entries are:
  - **all**—Dump static and dynamic entries from the PDB
  - **assigned**—Dump statically assigned proximity entries
  - **probed**—Dump dynamically probed proximity entries

  The default is **all**.

- **entry-address** *ip-address*—The IP address of the PDB entry.
- **netmask** *netmask*—The subnet mask of the PDB entry in dotted-decimal notation (for example, 255.255.255.0).

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

```
gss1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Starting Proximity Database dump.

gss1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump is in progress...
Proximity Database has dumped 15678 of 34512 entries

gss1.example.com# proximity database dump PDB2004_6_30 format xml
entry-type probed entry-address 172.23.5.7 netmask 255.255.255.255
Proximity Database dump completed. The number of dumped entries: 34512
```

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

Running a Periodic Proximity Database Backup

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

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

The syntax for this command is:

proximity database periodic-backup now

For example, enter:

```
gss1.example.com# proximity database periodic backup now
```

Loading Proximity Database Entries

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

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

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

The options and variable are:

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

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

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

```
gss1.example.com# proximity database load file GSS3PDB format binary
```

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

```
gss1.example.com# proximity database load GSS3PDB format binary
override
```

Initiating Probing for a D-proxy Address

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

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

The syntax for this command is:

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

The options and variables are:

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

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

```
gss1.example.com# proximity probe 172.16.5.7 zone 1
```

Disabling Proximity Locally on a GSS for Troubleshooting

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

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

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

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

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

```
gss1.example.com# proximity stop
```

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

```
gss1.example.com# proximity start
```