



Configuring DNS Sticky

This chapter describes how to configure a GSS to support Domain Name System (DNS) stickiness to answer requests received from client D-proxies. The GSS supports DNS sticky locally and also globally between GSS peers in the network.

This chapter contains the following major sections:

- [DNS Sticky Overview](#)
- [DNS Sticky Quick Start Guide](#)
- [Synchronizing the GSS System Clock with an NTP Server](#)
- [Configuring Sticky Using the Primary GSSM GUI](#)
- [Configuring Sticky Using the GSS CLI](#)
- [Disabling DNS Sticky Locally on a GSS for Troubleshooting](#)

**Note**

Each GSS supports a comprehensive set of **show** CLI commands to display sticky application mesh statistics for the device. In addition, the primary GSSM GUI displays sticky statistics for the GSS network. See [Chapter 10, Monitoring GSS Global Server Load-Balancing Operation](#), for details about viewing sticky statistics.

DNS Sticky Overview

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

For many users browsing a site, being redirected to a new site is transparent. However, customers performing e-commerce or other transactions may experience a break in the connection when redirected, which results in a loss of the e-commerce transaction. Having DNS sticky enabled on a GSS helps to ensure that e-commerce clients remain connected to a particular server for the duration of a transaction, even when the client's browser refreshes the DNS mapping.

While some browsers allow client connections to remain for the lifetime of the browser instance or for several hours, other browsers may impose a connection limit of 30 minutes before requiring a DNS re-resolution. This time period may not be long enough for a client to complete an e-commerce transaction. A new DNS resolution can then cause the client to connect to a server that is different from the original server, which can disrupt the transaction. DNS sticky helps to ensure that a client completes a transaction if a DNS re-resolution occurs.

This section contains the following topics on DNS sticky in the GSS:

- [Local DNS Sticky](#)
- [Sticky Database](#)
- [Global DNS Sticky](#)

Local DNS Sticky

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

Each GSS dynamically builds and maintains a local sticky database that is based on the answers that the GSS sends to the requesting client D-proxies. If a subsequent request comes from the same client D-proxy, and the answer in the database is valid, the GSS returns the cached answer to the client D-proxy.

You configure the GSS to perform sticky load-balancing operations through the configuration of options on DNS rules and balance clauses. You identify the sticky method used by the DNS rule by matching a hosted domain or matching a hosted domain list. When sticking on a domain, the GSS provides the same sticky answer to all requests from a client D-proxy for that domain. When sticking on a domain list, the GSS provides the same sticky answer to all requests from a client D-proxy for all domains in that domain list.

Before returning a sticky answer to a client, the GSS verifies the keepalive status. The resource responds as follows:

- If the resource is available (online state), the GSS uses this answer for the DNS response sent back to the D-proxy.
- If the resource is available (online state) but the VIP corresponding to the answer is overloaded, the GSS continues to use this answer for the DNS response sent back to the D-proxy. Sticky always takes precedence over an exceeded load threshold in the associated DNS rule.
- If the resource is unavailable (offline state), the GSS selects a new answer and inserts this answer into the sticky database, replacing the previous answer.

Sticky Database

The sticky database provides the core intelligence for all DNS sticky-based decisions made by a GSS, on a local or global level. The GSS collects requests from the client D-proxies and stores these requests in memory as the sticky database. Requests may be identified by the IP address of the client D-proxy or a database ID representing a list of D-proxy IP addresses (configured as a sticky group, see the [“Creating Sticky Groups”](#) section). The D-proxy IP address may also be some form of a sticky global netmask if the global subnet mask is set to a value other than the default of 255.255.255.255.

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

The primary GSSM supports the creation of sticky groups that allow you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its sticky database as a single entry. Instead of multiple sticky database entries, the GSS uses only one entry in the sticky database for multiple D-proxies. The GSS treats all D-proxies in a sticky group as a single D-proxy.

All entries in the sticky database age out respectively based on a user-specified global sticky inactivity timeout value. The sticky inactivity timeout value identifies the time period that an answer remains valid in the sticky database. Every time the GSS returns an answer to the requesting client, the GSS resets the expiration time of the answer to this value. When the sticky inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. You can specify a global sticky inactivity timeout default value for the GSS or modify the inactivity timeout value for each DNS rule.

**Note**

The sticky inactivity timeout is accurate to within 5 minutes of the specified value. Each entry persists in the sticky database for the configured sticky inactivity timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

Upon receiving a DNS request, the GSS looks in the sticky database for a matched entry based on the combination of D-proxy IP address (or sticky group ID) and requested hosted domain or domain list information in the request. If the GSS finds a matched entry (a hit), the GSS returns the original DNS answer to the requesting D-proxy and the GSS resets the user-configured sticky inactivity timeout to its starting value. If the GSS does not find a matched entry (a miss), the GSS does not return a sticky answer but, instead, performs normal load balancing for the request to locate a new answer and add the new entry into the sticky database.

The GSS supports a maximum of 400,000 entries in the sticky database. When the total number of entries in the sticky database reaches 400,000, the GSS automatically removes entries from the database based on the lowest percentage of time remaining.

Global DNS Sticky

This section provides an overview of the global DNS sticky function and the behavior of GSS devices operating in a peer mesh. It contains the following topics:

- [GSS Sticky Peer Mesh](#)
- [Sticky Mesh Conflict Resolution](#)
- [Communicating in the Sticky Peer Mesh](#)

GSS Sticky Peer Mesh

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

When one GSS device in the mesh receives a query from a client for a hosted domain or domain list, global sticky enables each GSS in the network to make a best effort attempt to return the same answer to the requesting client. This action is performed regardless of which GSS in the network is selected to answer the first and subsequent requests. The individual GSS devices work together to maintain a global sticky database across the network.

Each GSS in the peer mesh receives updates from the other peers and sends local changes to its remote peers. The GSS devices share the following information with the other GSS devices in the peer mesh:

- The sticky database lookups performed
- The persistent answers provided in the response
- The related time stamp and sticky inactivity timeout details

Each GSS communicates updates to its remote GSS peers when any of the following situations occur:

- A D-proxy request arrives at a GSS with no previous database entry. The GSS returns a new answer to the requesting client and enters that answer in its local database.
- A GSS returns a previous answer to the requesting client. The GSS resets the expiration time for the answer to its original sticky inactivity timeout value.
- The GSS finds an existing answer in the sticky database but a keepalive determines that the answer is nonresponsive (offline). In this case, the GSS uses the DNS rule to choose a new answer, overriding the previous answer in the sticky database, and communicates this answer to all peers.
- You use the **sticky database delete** CLI command to delete one or more entries from the sticky database.

A GSS does not send information to its peers when purging an answer from the sticky database due to reaching the normal sticky inactivity timeout or a sticky database overflow. It is expected that each GSS in the mesh performs this task independently.

When a local GSS node receives information from one of its peers in the network, that GSS performs a lookup of each received data entry in its local sticky database. Based on the results of the lookup, the GSS performs one of the following actions:

- If the GSS does not find the entry in its sticky database, the GSS adds the answer to its local sticky database.
- If the GSS finds the same entry in its sticky database, the GSS resets the expiration time for the answer to the initial sticky inactivity timeout value.

The GSS supports encryption of all inter-GSS communications to maintain the integrity of the sticky database information transferred among the mesh peers. Each GSS uses the Message Digest 5 (MD5)-based hashing method to encrypt the application data sent throughout the mesh.

To authenticate communication between GSS devices in the mesh to prevent unauthorized device access, you can specify a secret string that is used by all GSS devices in the mesh. The secret string provides a key for authentication between GSS devices as well as for encryption (if enabled). Each local GSS uses the Challenge Handshake Authentication Protocol (CHAP) method to establish a connection with a remote peer.

Sticky Mesh Conflict Resolution

In some instances, two or more GSS devices in the mesh may answer the same sticky request at the same time. When the GSS devices communicate their updates to each peer, the recipient detects a conflict. Conflicts are resolved in the peer network by each GSS keeping the record with the greatest expiration time stamp (that is, the newest record). If the conflicting entries have identical time stamps, the GSS uses the entry that contains the most recently configured answer based on the configuration ID.

Conflicts are far more likely to occur when multiple requests are grouped by domain list, or when you group D-proxy clients by a sticky mask or by sticky group. For example, if you configure a DNS rule for domains A and B, one client may request GSS 1 for domain A, while a second client may make a request for domain B. If the GSS receives both requests at the same time, the two clients may receive different answers.

You can reduce global sticky mesh conflicts if you do the following:

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

Communicating in the Sticky Peer Mesh

You can successfully pass packets between GSS peers in the sticky mesh by ensuring that the following requirements are met:

- Synchronize the system clock of each GSS device in the mesh with a Network Time Protocol (NTP) server. If the clock of a GSS device is out of synchronization with the other GSS peers (greater than a 3 minute difference), that GSS ignores update messages from other GSS devices until you synchronize its system clock. See the [“Synchronizing the GSS System Clock with an NTP Server”](#) section for details.
- Each GSS in the peer mesh has the same global subnet mask values. A GSS will drop all global sticky messages received from a GSS with a different subnet mask. A difference in global sticky masks on a peer would occur only if a configuration change was made on the primary GSSM GUI and the peer did not receive the change due to a network failure. See the [“Configuring DNS Sticky”](#) section for details.
- Each GSS in the peer mesh has the same version of GSS software.

If these conditions are not met, a GSS cannot properly receive or send packets with the other GSS peers in the sticky mesh.

A GSS leaves and rejoins the global sticky mesh when you perform one of the following actions:

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

Upon reentry into the mesh, the GSS attempts to load the sticky database from a peer GSS. The GSS uses the shortest round-trip time (RTT) to prioritize from which peer to request the database update. If a GSS peer is unavailable, the GSS locally restores the sticky database from the last available periodic database dump file. The GSS restores the sticky database from the database dump file any time it rejoins the mesh and cannot retrieve a database from a GSS peer in the mesh. When the load is complete, the local database on the GSS device contains a full version of the sticky database.

If you want the local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, you can identify a favored GSS peer for that GSS device. By identifying a favored GSS peer, you can also reduce network issues with peer synchronization, which typically generates a burst of network traffic. In this case, you direct network traffic to a different peer other than the GSS identified as being the closest (with the shortest round-trip time).

When you identify a favored peer, upon reentry into the mesh, the local GSS node always attempts to first synchronize its sticky database entries with the favored GSS peer. If the GSS peer is unavailable, the local GSS node queries the remaining mesh peers to find the closest up-to-date sticky database.

Network connectivity issues, GSS devices leaving and rejoining the mesh, and GSS device restarts have a minor impact on the synchronization of the sticky database. Sticky database entries always reconverge based on their usage and the user-configurable sticky inactivity timeout values.

DNS Sticky Quick Start Guide

[Table 8-1](#) provides a quick overview of the steps required to configure the GSS for DNS sticky operation, both local and global DNS sticky. Each step includes the primary GSSM GUI page or the GSS CLI command required to complete the task. For the procedures to configure the GSS for DNS sticky, see the sections following the table.

Table 8-1 DNS Sticky Configuration Quick Start

Task and Command Example

1. If you are using global sticky with multiple GSS devices, log in to the CLI of each GSS in the mesh, enable privileged EXEC mode, and synchronize its system clock with an NTP server.

For example, enter:

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

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

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

Task and Command Example

5. Modify one or more of the DNS sticky configuration default settings in the Global Sticky Configuration details page by performing the following steps:
 - a. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses. Use this parameter to increase the number of D-proxies supported in the sticky database by grouping multiple D-proxies into a single database entry. Enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit-count notation (for example, /24).
 - b. In the Entry Inactivity Timeout field, enter the maximum time interval, in minutes, for which an unused entry (answer) remains valid in the sticky database. This entry is the global default for the GSS. However, you can modify the inactivity timeout value for each DNS rule. Every time the GSS returns an answer to the requesting client, the GSS resets the expiration time of the answer to this value. When the sticky inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database.
 6. Configure inter-GSS global sticky mesh settings in the Global Sticky Configuration details page by performing the following steps:
 - a. At the Mesh Encryption option, enable or disable the encryption of data transmitted by GSS devices in the mesh. The GSS support encryption of all inter-GSS communications to maintain the integrity of the sticky database information transferred among the mesh peers.
 - b. To authenticate communication between GSS devices in the mesh to prevent unauthorized device access, enter a secret string in the Encryption String field. The secret string provides a key for authentication between GSS devices as well as for encryption (if enabled).
 - c. If you want a local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, in the Favored Peers section identify a favored peer for each local GSS node in the mesh.
 7. Click the **Submit** button to save your DNS sticky configuration changes.
-

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

Task and Command Example

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

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

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

Task and Command Example

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

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

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

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

Synchronizing the GSS System Clock with an NTP Server

If you are using global sticky in your GSS network, you must synchronize the clocks of all GSS devices in the mesh for a GSS to communicate with the other GSS devices in the peer mesh. If the clock of a GSS device is out of synchronization with the other GSS peers (by a value greater than 3 minutes), that GSS will ignore update messages from other GSS devices until you synchronize its system clock.

**Note**

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

You must specify the NTP server(s) for each GSS device that operates in the global mesh before you enable DNS sticky for those devices from the primary GSSM GUI. This sequence ensures that the clocks of each GSS device are synchronized before they join the global sticky peer mesh.

**Note**

For details on logging in to a GSS device and enabling privileged EXEC mode at the CLI, see the [“Logging in to the CLI and Enabling Privileged EXEC Mode”](#) section.

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

```
ntp-server ip_or_host
```

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

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

ntp enable

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

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

Configuring Sticky Using the Primary GSSM GUI

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

- [Configuring DNS Sticky](#)
- [Configuring the Global Sticky Mesh](#)
- [Enabling Sticky in a DNS Rule](#)

Configuring DNS Sticky

The GSS includes a set of DNS sticky settings that function as the default values used by the GSS network when you enable sticky in a DNS rule. You can configure sticky only in a DNS rule that uses a VIP-type answer group. In addition, sticky is active for a DNS rule only when the following conditions exist:

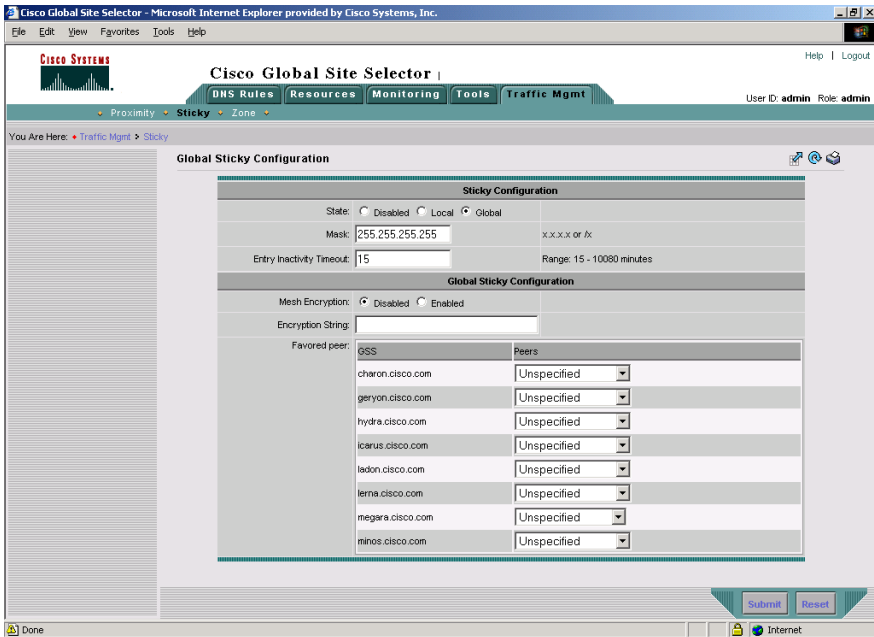
- Sticky is enabled for either global or local use. In the GUI, choose **Global** or **Local** for the State option in the Global Sticky Configuration details page.
- A sticky method option (domain or domain list) is selected. In the GUI, use the DNS Rule Builder and choose **By Domain** or **By Domain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

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

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

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

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



3. At the State option, click one of the following option buttons to enable or disable sticky for the GSS network:

- Disabled—Disables DNS sticky across the GSS network. When you disable sticky, the GSS answers DNS requests for all domains and clients, subject to DNS rule matching, without accessing the sticky database or sharing sticky database information between peers in the network.
 - Local—Enables DNS sticky for each active GSS device on a local level only. Each GSS attempts to ensure that subsequent requests for the same domain name are stuck to the same location as the first request. Sticky database information is not shared between GSS devices in the GSS mesh.
 - Global—Enables global DNS sticky for each active GSS device across the entire GSS mesh. With global DNS sticky, all local sticky features are in operation and each GSS device in your network shares answers between peer GSS devices in a peer mesh. The peer mesh attempts to ensure that if any GSS device in the mesh receives the same question, then the same answer is returned to the requesting client D-proxy.
4. In the Mask field, enter a global subnet mask that the GSS uses to uniformly group contiguous D-proxy addresses to increase the number of clients that the sticky database can support. Enter the subnet mask in either dotted-decimal notation (for example, 255.255.255.0) or as a prefix length in CIDR bit-count notation (for example, /24).

This mask is applied to the client source IP address before accessing the sticky database. The default global mask is 255.255.255.255.

When you define a DNS sticky group for incoming D-proxy addresses (see the “[Creating Sticky Groups](#)” section), if the incoming D-proxy address does not match any of the entries in a defined DNS sticky group, then the GSS uses this global netmask value to calculate a grouped D-proxy network address.

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

This value defines the sticky database entry age-out process. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database. The default value is 60 minutes.

The Inactivity Timeout value can also be set individually for each DNS rule. When you set an Inactivity Timeout value for a DNS rule, that value overrides the global Entry Inactivity Timeout value.

**Note**

The sticky inactivity timeout is accurate to within 5 minutes of the specified value. Each entry will persist in the sticky database for the configured sticky inactivity timeout value and may remain in the sticky database for no longer than 5 minutes past the specified value.

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

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

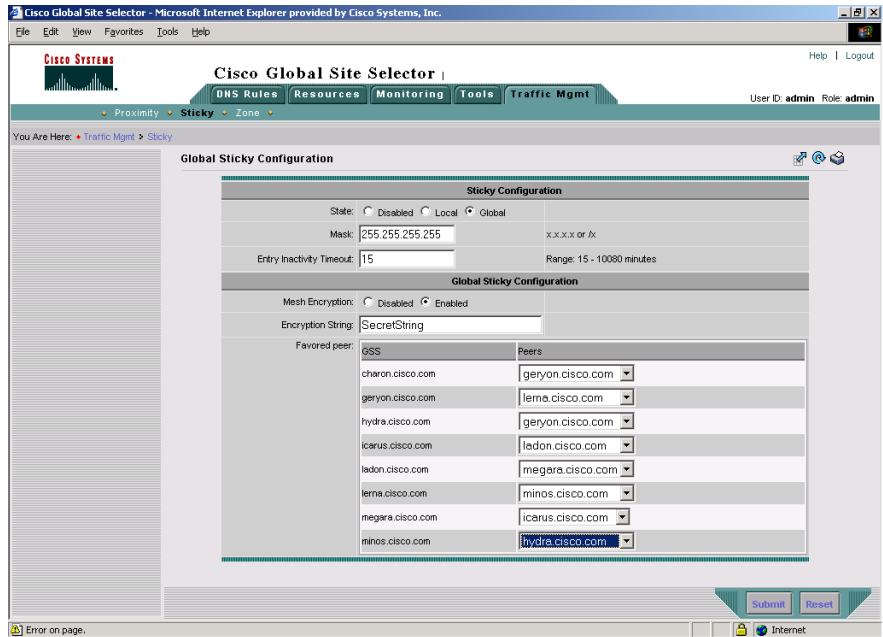
Configuring the Global Sticky Mesh

The GSS includes a set of parameters to configure inter-GSS global sticky mesh operation. You configure mesh operation through the Global Sticky Configuration details page of the Traffic Mgmt tab.

To configure the inter-GSS device mesh operation from the primary GSSM GUI, perform the following steps:

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

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



3. Ensure that you set the State option to **Global**.
4. At the Mesh Encryption option, enable or disable the encryption of data transmitted by GSS devices in the mesh. The GSS supports encryption of all inter-GSS communications throughout the mesh to maintain the integrity of the sticky database information transferred among the GSS peers as follows:
 - Disabled—Disables the encryption of data transferred between GSS peers in the mesh. The application data is transmitted in clear text.
 - Enabled—Enables the encryption of data transferred between GSS peers in the mesh. Each GSS uses the Message Digest 5 (MD5)-based hashing method to encrypt the application data sent throughout the mesh.
5. Authenticate communication between GSS peers in the mesh to prevent unauthorized device access by entering a secret string in the Encryption String field. Enter an unquoted text string with a maximum of 32 characters and no spaces.

The secret string provides a key for authentication between GSS peers as well as for encryption (if enabled). Each local GSS uses the Challenge Handshake Authentication Protocol (CHAP) method to establish a connection with a remote peer. You globally configure the shared secret on the primary GSSM GUI, which is used by all mesh peers.

6. If you want a local GSS node to attempt synchronization with a specific GSS peer upon reentry into the sticky mesh, in the Favored Peers section, identify a favored peer for each local GSS node in the mesh.

By identifying a favored GSS peer, you can also reduce network issues with peer synchronization, which typically generates a burst of network traffic. In this case, you can direct network traffic to a different peer other than the GSS identified as being the closest (with the shortest round-trip time). The Favored Peers section of the page presents an array of all local GSS nodes in the mesh along with a drop-down list of the remote peers.

A GSS joins the mesh upon one of the following:

- A reload.
- A power up.
- When you enter a **gss stop** and **gss start** CLI command sequence.
- When you enter a **gss reload** CLI command.
- When you enter a **sticky stop** and **sticky start** CLI command sequence.
- When you choose the **Global** state in the Global Sticky Configuration details page from either the Disabled or Local state.

Upon reentry into the mesh, the local GSS node first attempts to synchronize its sticky database entries with the favored GSS peer. If the favored peer is unavailable, the GSS queries the remaining mesh peers to find the closest up-to-date sticky database (with the shortest round-trip time).

For example, assume there are four GSS devices in a mesh (gss_1, gss_2, gss_3, and gss_4), and both gss_1 and gss_2 are in the bootup process. You can direct local node gss_1 to gss_3 as its favored peer, and direct local node gss_2 to gss_4 as its favored peer. The identification of favored peers in the mesh can prevent those GSS devices that are booting from waiting for another database request to complete before their database synchronization request can be serviced.

If you want a GSS to automatically query all mesh peers to find the closest up-to-date sticky database, leave the individual GSS device selection at **Unspecified**. The GSS uses the shortest round-trip time to prioritize which peers to request a database update.

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

Enabling Sticky in a DNS Rule

This section contains the following topics:

- [Sticky DNS Rule Overview](#)
- [Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups](#)



Note

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

Sticky DNS Rule Overview

After you enable DNS sticky from the Global Sticky Configuration details page, add stickiness to a DNS rule using the DNS Rule Builder. The GSS supports DNS stickiness in a DNS rule on either a matching domain (By Domain) or on a matching domain list (By Domain List). The By Domain and By Domain List sticky methods instruct the GSS that all requests from a client D-proxy for a matching hosted domain or domain list are to be given the same answer for the duration of a user-configurable sticky time period.

Enabling sticky in a DNS rule clause causes the GSS to look up in the sticky database for a matched entry based on a combination of D-proxy IP address and requested domain information, and, if the answer is found, to return the answer as the DNS response to the requesting D-proxy. If the answer is in the offline state, or the GSS does not find the answer, it evaluates the balance method clauses in the DNS rule to choose a new answer.

You can configure sticky individually for each balance clause in a DNS rule. However, the GSS prevents you from enabling sticky on Balance Clause 2 if you do not first enable sticky on Balance Clause 1. This restriction also applies if you attempt to enable sticky on Balance Clause 3 without first configuring sticky on Balance Clause 2.

**Note**

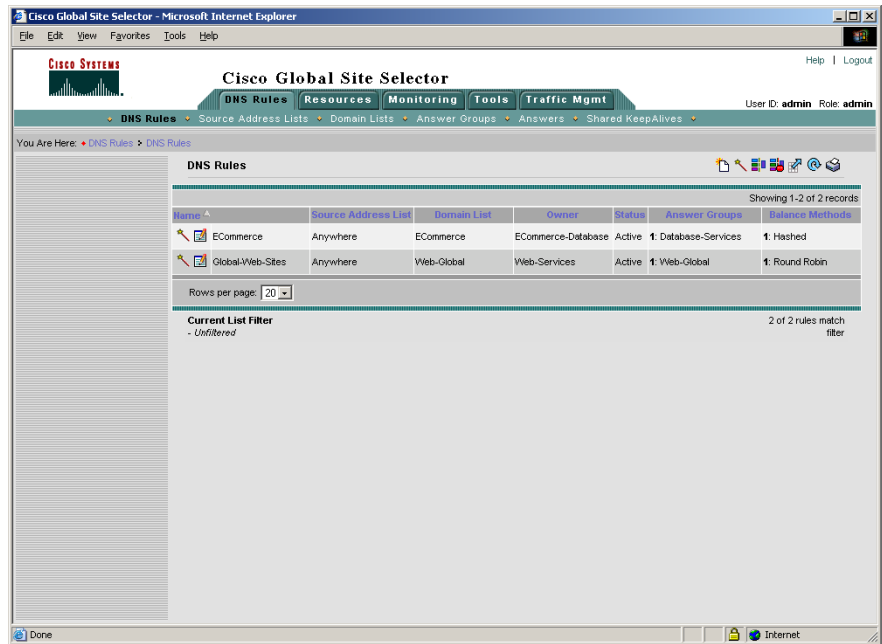
If you use DNS sticky and network proximity in your DNS rule, stickiness always takes precedence over proximity. When a valid sticky answer exists for a given DNS rule match, the GSS does not consider proximity when returning an answer to a client D-proxy.

Using the DNS Rule Builder to Add Sticky to a DNS Rule that use VIP-Type Answer Groups

To use the DNS Rule Builder to add sticky to a DNS rule that uses VIP-type answer groups, perform the following steps:

1. If you have not already done so, enable local or global DNS sticky using the Global Sticky Configuration details page of the Traffic Mgmt tab. See the [“Configuring DNS Sticky”](#) section for details.
2. From the primary GSSM GUI, click the **DNS Rules** tab, and then click the **DNS Rules** navigation link. The DNS Rules list page appears (see [Figure 8-3](#)).

Figure 8-3 DNS Rules List Page



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

Figure 8-4 Create New DNS Rule Window

4. Develop your DNS rule as outlined in steps 3 through 7 in the “[Building DNS Rules Using the DNS Rule Builder](#)” section of [Chapter 7, Building and Modifying DNS Rules](#).
5. Enable or disable sticky globally for the DNS rule, at the Select Sticky Method option, by choosing one of the following selections:
 - None—Disables DNS sticky across the GSS network for this DNS rule. When you disable sticky, the GSS answers DNS requests for all domains and clients that pertain to the DNS rule, subject to DNS rule matching, without accessing the sticky database or sharing sticky database information between peers in the network.

- **By Domain**—Enables DNS stickiness on a domain. For all requests from a single D-proxy, the GSS sends the same answer for a domain. For rules matching on a domain wildcard (for example, *.cisco.com), entries are stuck together using the global configuration ID assigned to the wildcard. The GSS does not attempt to distinguish the individual domains that match the wildcard.
 - **By Domain List**—Enables DNS stickiness on a matching domain list. The GSS groups all domains in the domain list and treats them as a single hosted domain. The GSS treats wildcards in domain lists the same as non-wildcard domains.
6. Override the global Entry Inactivity Timeout value set on the Global DNS Sticky details page (see the “[Configuring DNS Sticky](#)” section) for this DNS rule by specifying a value in the Inactivity Timeout field. Enter a value from 15 to 10080 minutes, defined in 5 minute intervals (15, 20, 25, 30, up to 10080).

Enter the maximum time interval that can pass without the sticky database receiving a lookup request for an entry. Every time the GSS returns an answer to the requesting client D-proxy, the GSS resets the expiration time of the answer to this value. When the sticky inactivity timeout value elapses without the client again requesting the answer, the GSS identifies the answer as invalid and purges it from the sticky database.

**Note**

The sticky inactivity timeout is accurate to within 5 minutes of the specified value. Each entry will persist in the sticky database for the configured sticky inactivity timeout value, and may remain in the sticky database for no longer than 5 minutes past the specified value.

7. At the Balance Clause 1 heading, perform the following:
- Choose the answer group component of your first answer group and balance method pairing from the drop-down list. This is the first effort the GSS uses to select an answer for the DNS query.
 - Choose the balance method for the answer group from the drop-down list.
 - Click the **Sticky Enable** check box to activate DNS sticky for the balance clause. This checkbox appears only when you enable sticky for the DNS rule at the Select Sticky Method option.

8. Complete your DNS rule as described in the “[Building DNS Rules Using the DNS Rule Builder](#)” section of [Chapter 7, Building and Modifying DNS Rules](#). Choose additional answer group and balance method pairings for Balance Clause 2 and Balance Clause 3.

**Note**

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

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

Configuring Sticky Using the GSS CLI

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

The section contains the following topics:

- [Logging in to the CLI and Enabling Privileged EXEC Mode](#)
- [Creating Sticky Groups](#)
- [Deleting Entries from the Sticky Database](#)
- [Dumping Sticky Database Entries](#)
- [Running a Periodic Sticky Database Backup](#)
- [Loading Sticky Database Entries](#)

Logging in to the CLI and Enabling Privileged EXEC Mode

**Note**

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

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

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

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

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

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

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

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

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

Creating Sticky Groups

The primary GSSM supports the creation of sticky groups. A sticky group allows you to configure multiple blocks of D-proxy IP addresses that each GSS device stores in its sticky database as a single entry. Instead of multiple sticky database entries, the GSS uses only one entry in the sticky database for multiple D-proxies. The GSS treats all D-proxies in a sticky group as a single D-proxy.

This section contains the following topics:

- [DNS Sticky Group Overview](#)
- [Creating a DNS Sticky Group](#)
- [Deleting a Sticky Group IP Address Block](#)
- [Deleting a Sticky Group](#)

DNS Sticky Group Overview

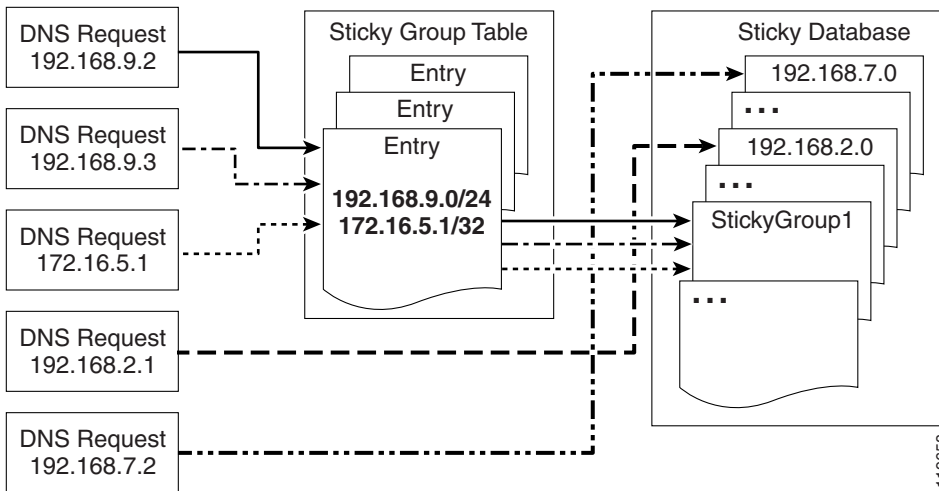
You create sticky groups from the primary GSSM CLI to obtain better scalability of your configuration and to allow easy sticky group creation through automated scripts. The primary GSSM supports a maximum of 800 sticky groups. Each sticky group contains one to 30 blocks of IP addresses and subnet masks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

Grouping D-proxy IP addresses in the sticky database allows you to address proxy hopping. Certain ISPs rotate their D-proxies. A user's browser may use DNS server A to resolve a hostname and later use DNS server B to resolve the same name. This technique is referred to as proxy hopping because the DNS sticky function remembers the client's D-proxy IP address and not the IP address of the actual client. In this case, rotating D-proxies appear to the GSS as unique clients. Sticky grouping allows you to globally group sets of D-proxies to solve this proxy hopping problem.

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

Figure 8-5 illustrates how through DNS sticky group entries 192.168.9.0 255.255.255.0 and 172.16.5.1 255.255.255.255, the DNS requests from D-proxies 192.168.9.2, 192.168.9.3 and 172.16.5.1 all map to the identified group name, *StickyGroup1*. If no match is found in the sticky group table for an incoming D-proxy IP address, the GSS applies a user-specified global netmask to calculate a network address as the database key. In this example, DNS requests from 192.168.2.1 and 192.168.7.2 use the database entries keyed as 192.168.2.0 and 192.168.7.0 with a specified global netmask of 255.255.255.0.

Figure 8-5 Locating a Grouped Sticky Database Entry



Creating a DNS Sticky Group

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

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

The syntax for this command is as follows:

```
sticky group groupname ip ip-address netmask netmask
```

The arguments and keywords are as follows:

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

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

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

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

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

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

Deleting a Sticky Group IP Address Block

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

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no sticky group StickyGroup1 ip
192.168.3.0 netmask 255.255.255.0
```

Deleting a Sticky Group

You can delete a sticky group by using the **no** form of the **sticky group** command. For example, enter:

```
gssm1.example.com# config
gssm1.example.com(config)# gslb
gssm1.example.com(config-gslb)# no sticky group StickyGroup1
```

Deleting Entries from the Sticky Database

You can remove entries from the sticky database of each GSS device by using the **sticky database delete** CLI command. When operating in a global sticky configuration, the result of the **sticky database delete** command propagates throughout the GSS mesh to maintain synchronization between the peers in the GSS network.



Caution

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

To view the entries in the sticky database to identify the sticky entries that you want to delete, use the **show sticky database** command (see the “[Displaying the Sticky Database Status](#)” section in [Chapter 10, Monitoring GSS Global Server Load-Balancing Operation](#)).

Use the **sticky database delete** command to remove entries from the sticky database. The syntax for this command is as follows:

```
sticky database delete { all | answer { name/ip_address } | domain { name } |
domain-list { name } | group { name } | inactive minimum { minutes }
maximum { minutes } | ip { ip_address } netmask { netmask } | rule
{ rule_name }
```

The keywords and arguments are as follows:

- **all**—Removes all entries from the sticky database memory. The prompt “Are you sure?” appears to confirm the deletion of all database entries. Specify **y** to delete all entries or **n** to cancel the deletion operation.
- **answer** *name/ip_address*—Removes all sticky entries related to a particular answer. Specify the name of the answer. If there is no name for the answer, specify the IP address of the sticky answer in dotted-decimal notation (for example, 192.168.9.0).
- **domain** *name*—Removes all sticky entries related to a domain. Specify the exact name of a previously created domain.
- **domain-list** *name*—Removes all sticky entries related to a domain list. Specify the exact name of a previously created domain list.
- **group** *name*—Removes all sticky entries related to a sticky group. Specify the exact name of a previously created sticky group.
- **inactive minimum** *minutes* **maximum** *minutes*—Removes all sticky entries that have not received a lookup request by a client D-proxy in the specified minimum and maximum time interval. If you do not specify a maximum value, the GSS deletes all entries that have been inactive for the specified minimum value or longer. The GSS returns an error if one of the following situations occur:
 - The maximum value is set to a value that is less than the minimum value.
 - The minimum and maximum values are not within the allowable range of values for the sticky inactivity timeout.

Valid entries are 0 to 10100 minutes.

- **ip** *ip_address netmask netmask*—Removes all sticky entries related to a D-proxy IP address and subnet mask. Specify the IP address of the requesting client's D-proxy in dotted-decimal notation (for example, 192.168.9.0) and specify the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- **rule** *rulename*—Removes all sticky entries related to a DNS rule. Specify the exact name of a previously created DNS rule.

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

```
gss1.example.com# sticky database delete ip 192.168.8.0 netmask
255.255.255.0
```

Dumping Sticky Database Entries

The GSS automatically dumps sticky database entries to a backup file on disk approximately every 20 minutes. The GSS uses this backup file to initialize the sticky database upon system restart or reboot to enable the GSS to recover the contents of the database. When global sticky is enabled, the GSS restores from the database dump file any time it reenters the mesh and cannot retrieve the sticky database contents from a GSS peer in the mesh.

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

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

The GSS includes options that provide a level of granularity for dumping entries from the sticky database. The GSS supports binary and XML output formats. Optionally, you can specify the entry type filter to clarify the information dumped from the sticky database.

If you do specify a format but do not specify an entry type, the GSS automatically dumps all entries from the sticky database.

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

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

Use the **sticky database dump** command to output entries from the sticky database. The syntax for this command is as follows:

```
sticky database dump {filename} format {binary | xml} entry-type {all | group | ip}
```

The arguments and variables are as follows:

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



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

- **entry-type**—Specifies the type of sticky database entries to dump. The valid entries are as follows:
 - **all**—Dumps all entries from the sticky database
 - **group**—Dumps all entries that have sticky group IDs from the database
 - **ip**—Dumps all entries that have source IP addresses from the database

This example shows how to dump the D-proxy source IP addresses from the sticky database to the `sdb2004_06_30` file in XML format. If the dump is large, progress messages appear.

```
gss1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Starting Sticky Database dump.

gss1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump is in progress...
Sticky Database has dumped 15678 of 34512 entries

gss1.example.com# sticky database dump sdb2004_06_30 format xml
entry-type ip
Sticky Database dump completed. The number of dumped entries: 34512
gss1.example.com#
```

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

Running a Periodic Sticky Database Backup

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

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

The syntax for this command is as follows:

```
sticky database periodic-backup now
```

For example, enter:

```
gss1.example.com# sticky database periodic-backup now
```

Loading Sticky Database Entries

The GSS supports the loading and merging of sticky database entries from a file into the existing sticky database in GSS memory. The sticky database merge capability supports the addition of entries from one GSS into another GSS. The file must be in binary format for loading into GSS memory.

The GSS validates the loaded database entries, checks the software version for compatibility, and then adds the sticky database entries in memory. The GSS does not overwrite existing, duplicate entries in the sticky database.

Use the **sticky database load** command to load and merge a sticky database from disk into the existing sticky database in GSS memory. The syntax for this command is as follows:

```
sticky database load filename
```



Note

If you want to load and replace all sticky database entries from a GSS instead of merging the entries with the existing sticky database, enter the **sticky database delete all** command to remove all entries from the sticky database memory before you enter the **sticky database load** command.

Specify the name of the sticky database file to load and merge with the existing sticky database on the GSS device. The file must be in binary format for loading into GSS memory (see the [“Dumping Sticky Database Entries”](#) section). Use the **ftp** command in EXEC or global configuration mode to launch the FTP client and transfer the sticky database file to the GSS from a remote GSS.

This example shows how to load and merge the entries from the GSS3SDB file with the existing entries in the GSS sticky database:

```
gss1.example.com# sticky database load GSS3SDB
```

Disabling DNS Sticky Locally on a GSS for Troubleshooting

You can disable DNS sticky for a single GSS when you need to locally override the GUI-enabled sticky option. You may need to locally disable sticky on a GSS when you need to troubleshoot or debug the device. The GSS does not store the local-disable setting in its running-configuration file. When you restart the device and sticky has been enabled from the primary GSSM GUI, the GSS reenables DNS sticky.

Use the **sticky stop** and **sticky start** commands to locally override the sticky enable option of the primary GSSM GUI.

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

- Sticky lookups in the sticky database
- Accessing the sticky database for new requests
- Periodic sticky database dumps
- The sticky database entry age-out process

The GSS continues to answer DNS requests according to the DNS rules and keepalive status.

When you locally disable sticky on a GSS, sticky remains disabled until you perform one of the following actions:

- Enter the **sticky start** CLI command.
- Enter the **gss restart** CLI command to restart the GSS software.
- Enter the **gss reload** CLI command to perform a cold restart of the GSS device.

If you are using global DNS sticky in your network, upon reentry of the GSS device into the peer mesh, the GSS attempts to synchronize the database entries with the other peers in the mesh. The GSS queries each peer to find the closest up-to-date sticky database. If no update is available from a peer, the GSS initializes the sticky database entries from the previously saved database on disk if a file is present and valid. Otherwise, the GSS starts with an empty sticky database.

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

```
gss1.example.com# sticky stop
```

This example shows how to locally reenable DNS on the GSS device using the **sticky start** command:

```
gss1.example.com# sticky start
```