How to Configure IOS SLB Features

Last Updated: April 26, 2011

Configuring IOS SLB involves identifying server farms, configuring groups of real servers in server farms, and configuring the virtual servers that represent the real servers to the clients.

For configuration examples associated with these tasks, see the “Configuration Examples for IOS SLB” section.

For a complete description of the IOS SLB commands in this section, refer to the “Server Load Balancing Commands” chapter of the *Cisco IOS IP Application Services Command Reference*. To locate documentation of other commands that appear in this section, search online using Cisco.com.

- How to Configure Required and Optional IOS SLB Functions, page 2
- How to Configure Firewall Load Balancing, page 12
- How to Configure a Probe, page 19
- How to Configure DFP, page 28
- GPRS Load Balancing Configuration Task List, page 29
- GGSN-IOS SLB Messaging Task List, page 31
- How to Configure GPRS Load Balancing Maps, page 32
- How to Configure KAL-AP Agent Support, page 34
- RADIUS Load Balancing Configuration Task List, page 36
- Exchange Director for mSEF Configuration Task List, page 43
- VPN Server Load Balancing Configuration Task List, page 52
- ASN Load Balancing Configuration Task List, page 53
- Home Agent Director Configuration Task List, page 54
- How to Configure NAT, page 55
- How to Configure Static NAT, page 56
- Stateless Backup Configuration Task List, page 57
- Stateful Backup of Redundant Route Processors Configuration Task List, page 58
- How to Configure Database Entries, page 59
- How to Configure Buffers for the Fragment Database, page 60
- How to Clear Databases and Counters, page 60

- How to Configure a Wildcard Search, page 62
- How to Configure Protocol-Level Purging of MLS Entries, page 62
- How to Purge and Reassign Connections, page 63
- How to Disable Automatic Server Failure Detection, page 64
- How to Monitor and Maintain the Cisco IOS SLB Feature, page 65

How to Configure Required and Optional IOS SLB Functions

To configure IOS SLB functions, perform the tasks in the following sections. Required and optional tasks are indicated.

- How to Configure a Server Farm and a Real Server, page 2
- How to Configure a Virtual Server, page 5
- How to Verify a Virtual Server, page 11
- How to Verify a Server Farm, page 11
- How to Verify Clients, page 12
- How to Verify IOS SLB Connectivity, page 12

How to Configure a Server Farm and a Real Server

Perform this required task to configure a server farm and a real server.

Note You cannot configure IOS SLB from different user sessions at the same time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **access** *interface*
5. **bindid** [*bind-id*]
6. **nat** {**client** *pool* | **server**}
7. **predictor** [**roundrobin**| **leastconns**| **route-map** *mapname*]
8. **probe** *probe*
9. **real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*]
10. **faildetect numconns** *number-of-conns* [**numclients** *number-of-clients*]
11. **maxclients** *number-of-conns*
12. **maxconns** *number-of-conns* [**sticky-override**]
13. **reassign** *threshold*
14. **retry** *retry-value*
15. **weight** *setting*
16. **inservice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb serverfarm** *server-farm* **Example:** `Router(config)# ip slb serverfarm PUBLIC`	Adds a server farm definition to the IOS SLB configuration and enters server farm configuration mode.
Step 4	**access** *interface* **Example:** `Router(config-slb-sfarm)# access GigabitEthernet 0/1.1`	(Optional) Configures an access interface or subinterface for a server farm.
Step 5	**bindid** [*bind-id*] **Example:** `Router(config-slb-sfarm)# bindid 309`	(Optional) Specifies a bind ID on the server farm for use by Dynamic Feedback Protocol (DFP). **Note** GPRS load balancing and Home Agent Director do not support this command.
Step 6	**nat** {**client** *pool* | **server**} **Example:** `Router(config-slb-sfarm)# nat server`	(Optional) Configures Network Address Translation (NAT) client translation mode or NAT server address translation mode on the server farm. All IPv4 or IPv6 server farms that are associated with the same virtual server must have the same NAT configuration.
Step 7	**predictor** [**roundrobin**| **leastconns**| **route-map** *mapname*] **Example:** `Router(config-slb-sfarm)# predictor leastconns`	(Optional) Specifies the algorithm to be used to determine how a real server is selected. **Note** RADIUS load balancing requires the default setting (the weighted round robin algorithm). In GPRS load balancing without GTP cause code inspection enabled, you must accept the default setting (the weighted round robin algorithm). The Home Agent Director requires the default setting (the weighted round robin algorithm). When you specify the **predictor route-map** command in SLB server farm configuration mode, no further commands in SLB server farm configuration mode or real server configuration mode are allowed. For more details, see the following sections: • "Weighted Round Robin Algorithm"

	Command or Action	Purpose
		• "Weighted Least Connections Algorithm" • "Route Map Algorithm"
Step 8	**probe** *probe* **Example:** `Router(config-slb-sfarm)# probe PROBE1`	(Optional) Associates a probe with the real server.
Step 9	**real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*] **Example:** `Router(config-slb-sfarm)# real 10.1.1.1`	Identifies a real server by IPv4 address, and optional IPv6 address and port number, as a member of a server farm and enters real server configuration mode. **Note** In GPRS load balancing, specify the IP addresses (virtual template addresses, for Cisco GGSNs) of the real servers performing the GGSN function. In VPN server load balancing, specify the IP addresses of the real servers acting as VPN terminators. For the Home Agent Director, specify the IP addresses of the real servers acting as home agents. For dual-stack support for GTP load balancing, specify the real server's IPv4 and IPv6 address.
Step 10	**faildetect numconns** *number-of-conns* [**numclients** *number-of-clients*] **Example:** `Router(config-slb-real)# faildetect numconns 10 numclients 3`	(Optional) Specifies the number of consecutive connection failures and, optionally, the number of unique client connection failures, that constitute failure of the real server. • In GPRS load balancing, if only one SGSN is configured in your environment, specify the **numclients** keyword with a value of 1. • In RADIUS load balancing, for automatic session-based failure detection, specify the **numclients** keyword with a value of 1.
Step 11	**maxclients** *number-of-conns* **Example:** `Router(config-slb-real)# maxclients 10`	(Optional) Specifies the maximum number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server.
Step 12	**maxconns** *number-of-conns* [**sticky-override**] **Example:** `Router(config-slb-real)# maxconns 1000`	(Optional) Specifies the maximum number of active connections allowed on the real server at one time.
Step 13	**reassign** *threshold* **Example:** `Router(config-slb-real)# reassign 2`	(Optional) Specifies the threshold of consecutive unacknowledged SYNchronize sequence numbers (SYNs) or Create Packet Data Protocol (PDP) requests that, if exceeded, result in an attempted connection to a different real server. **Note** In GPRS load balancing, you must specify a reassign threshold less than the SGSN's N3-REQUESTS counter value.
Step 14	**retry** *retry-value*	(Optional) Specifies the time interval, in seconds, to wait between the detection of a server failure and the next attempt to connect to the failed server.

	Command or Action	Purpose
	Example: `Router(config-slb-real)# retry 120`	
Step 15	**weight** *setting* **Example:** `Router(config-slb-real)# weight 24`	(Optional) Specifies the real server workload capacity relative to other servers in the server farm. **Note** If you use Dynamic Feedback Protocol (DFP), the static weights you define using the weight command in server farm configuration mode are overridden by the weights calculated by DFP. If DFP is removed from the network, IOS SLB reverts to the static weights.
Step 16	**inservice** **Example:** `Router(config-slb-real)# inservice`	Enables the real server for use by IOS SLB.

Note When performing server load balancing and firewall load balancing together on a Cisco Catalyst 6500 Family Switch, use the **mls ip slb wildcard search rp** command to reduce the probability of exceeding the capacity of the Telecommunications Access Method (TCAM) on the Policy Feature Card (PFC). See "How to Configure a Wildcard Search" for more details.

How to Configure a Virtual Server

Perform this required task to configure a virtual server. IOS SLB supports up to 500 virtual servers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb vserver** *virtual-server*
4. Do one of the following:
   - **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] {**esp**| **gre**| *protocol*}
   -
   -
   - **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*]
5. **serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]
6. **access** *interface* [**route framed-ip**]
7. **advertise** [**active**]
8. **client** {*ipv4-address netmask*[**exclude**] | **gtp carrier-code** [*code*]}
9. **delay** {*duration* | **radius framed-ip** *duration*}
10. **gtp notification cac** [*reassign-count*]
11. **gtp session**
12. **gw port** *port*
13. **hand-off radius** *duration*
14. **idle** [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*]
15. **purge radius framed-ip acct on-off**
16. **purge radius framed-ip acct stop** {*attribute-number* | {**26**| *vsa*} {*vendor-ID* | **3gpp**| **3gpp2**} *sub-attribute-number*}
17. **radius acct local-ack key** [*encrypt*] *secret-string*
18. **radius inject auth** *group-number* {**calling-station-id** | **username**}
19. **radius inject auth timer** *seconds*
20. **radius inject auth vsa** *vendor-id*
21. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string timeout*]
22. **replicate interval** *interval*
23. **replicate slave**
24. **sticky** {*duration*[**group** *group-id*] [**netmask** *netmask*] | **asn msid**[**group** *group-id*] | **gtp imsi**[**group** *group-id*] | **radius calling-station-id**| **radius framed-ip**[**group** *group-id*] | **radius username**[**msid-cisco**] [**group** *group-id*]}
25. **synguard** *syn-count interval*
26. **inservice** [**standby** *group-name*] [**active**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb vserver** *virtual-server* **Example:** `Router(config)# ip slb vserver PUBLIC_HTTP`	Identifies a virtual server and enters virtual server configuration mode.
Step 4	Do one of the following: • **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] {**esp**| **gre**| *protocol*} • • • **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*] **Example:** `Router(config-slb-vserver)# virtual 10.0.0.1 tcp www`	Specifies the virtual server IP address, type of connection, and optional TCP or User Datagram Protocol (UDP) port number, Internet Key Exchange (IKE) or Wireless Session Protocol (WSP) setting, and service coupling. **Note** For RADIUS load balancing, specify the **service radius** keyword option. **Note** For ASN load balancing, specify the **service asn** keyword option. **Note** For GPRS load balancing: • ◦ Specify a virtual GGSN IP address as the virtual server, and specify the **udp** keyword option. ◦ To load-balance GTP v1 and GTP v2 sessions, specify port number 2123, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports). ◦ To load-balance GTP v0 sessions, specify port number 3386, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any** to configure an all-port virtual server. ◦ To enable GPRS load balancing *without* GTP cause code inspection, specify the **service gtp** keyword option. ◦ To enable GPRS load balancing *with* GTP cause code inspection, specify the **service gtp-inspect** keyword option. ◦ For dual-stack support for GTP load balancing, specify the virtual server's IPv4 and IPv6 addresses and optional IPv6 prefix.
Step 5	**serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-*	Associates a real server farm with a virtual server, and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm.

	Command or Action	Purpose
	farm[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] **Example:** `Router(config-slb-vserver)# serverfarm SF1 backup SF2 map 1 priority 1`	**Note** RADIUS load balancing and the Home Agent Director do not support the **sticky** keyword. You can associate more than one server farm with a given RADIUS virtual server by configuring more than one **serverfarm** command, each with a unique map ID and a unique priority. (That is, each map ID and each map priority must be unique across all server farms associated with the virtual server.) For GPRS load balancing, if a real server is defined in two or more server farms, each server farm must be associated with a different virtual server. For dual-stack support for GTP load balancing, specify the primary IPv6 server farm and optional backup IPv6 server farm. All IPv4 or IPv6 server farms that are associated with the same virtual server must have the same NAT configuration.
Step 6	**access** *interface* [**route framed-ip**] **Example:** `Router(config-slb-vserver)# access Vlan20 route framed-ip`	(Optional) Enables framed-IP routing to inspect the ingress interface.
Step 7	**advertise** [**active**] **Example:** `Router(config-slb-vserver)# advertise`	(Optional) Controls the installation of a static route to the Null0 interface for a virtual server address.
Step 8	**client** {*ipv4-address netmask*[**exclude**] | **gtp carrier-code** [*code*]} **Example:** `Router(config-slb-vserver)# client 10.4.4.0 255.255.255.0`	(Optional) Specifies which clients are allowed to use the virtual server. **Note** GPRS load balancing supports only the **gtp carrier-code** option, and only if GTP cause code inspection is enabled. Dual-stack support for GTP load balancing does not support this command.
Step 9	**delay** {*duration* | **radius framed-ip** *duration*} **Example:** `Router(config-slb-vserver)# delay 30`	(Optional) Specifies the time IOS SLB maintains TCP connection context after a connection has ended.
Step 10	**gtp notification cac** [*reassign-count*] **Example:** `Router(config-slb-vserver)# gtp notification cac 5`	(Optional) Limits the number of times IOS SLB can reassign a session to a new real server for GGSN-IOS SLB messaging.
Step 11	**gtp session** **Example:** `Router(config-slb-vserver)# no gtp session`	(Optional) Enables IOS SLB to create GTP load-balancing sessions. This is the default setting. To enable sticky-only load balancing for GTP, use the **no** form of this command: **no gtp session**

	Command or Action	Purpose
		If you enable sticky-only load balancing, you must also enable sticky connections for the virtual server using the **sticky (virtual server)**command.
Step 12	**gw port** *port* **Example:** `Router(config-slb-vserver)# gw port 63082`	(Optional) Specifies the port that the Cisco Broadband Wireless Gateway (BWG) is to use to communicate with IOS SLB.
Step 13	**hand-off radius** *duration* **Example:** `Router(config-slb-vserver)# hand-off radius 30`	(Optional) Changes the amount of time IOS SLB waits for an ACCT-START message from a new Mobile IP foreign agent in the event of a foreign agent hand-off.
Step 14	**idle** [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*] **Example:** `Router(config-slb-vserver)# idle 120`	(Optional) Specifies the minimum time IOS SLB maintains connection context in the absence of packet activity. **Note** In GPRS load balancing *without* GTP cause code inspection enabled, specify an idle timer greater than the longest possible interval between PDP context requests on the SGSN.
Step 15	**purge radius framed-ip acct on-off** **Example:** `Router(config-slb-vserver)# purge radius framed-ip acct on-off`	(Optional) Enables IOS SLB to purge entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting On or Off message.
Step 16	**purge radius framed-ip acct stop** {*attribute-number* | {**26**| *vsa*} {*vendor-ID* | **3gpp**| **3gpp2**} *sub-attribute-number*} **Example:** `Router(config-slb-vserver)# purge radius framed-ip acct stop 44`	(Optional) Enables IOS SLB to purge entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting-Stop message.
Step 17	**radius acct local-ack key** [*encrypt*] *secret-string* **Example:** `Router(config-slb-vserver)# radius acct local-ack key SECRET_PASSWORD`	(Optional) Enables a RADIUS virtual server to acknowledge RADIUS accounting messages.
Step 18	**radius inject auth** *group-number* {**calling-station-id** | **username**}	(Optional) Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and specifies whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames.

	Command or Action	Purpose
	Example: `Router(config-slb-vserver)# radius inject auth 1 calling-station-id`	
Step 19	**radius inject auth timer** *seconds* **Example:** `Router(config-slb-vserver)# radius inject auth timer 45`	(Optional) Configures a timer for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
Step 20	**radius inject auth vsa** *vendor-id* **Example:** `Router(config-slb-vserver)# radius inject auth vsa vendor1`	(Optional) Buffers VSAs for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
Step 21	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string timeout*] **Example:** `Router(config-slb-vserver)# replicate casa 10.10.10.11 10.10.11.12 4231`	(Optional) Configures a stateful backup of IOS SLB decision tables to a backup switch. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate casa** command is not supported (because sessions are not persistent, and there is nothing to replicate).
Step 22	**replicate interval** *interval* **Example:** `Router(config-slb-vserver)# replicate interval 20`	(Optional) Sets the replication delivery interval for an IOS SLB virtual server. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate casa** command is not supported (because sessions are not persistent, and there is nothing to replicate).
Step 23	**replicate slave** **Example:** `Router(config-slb-vserver)# replicate slave`	(Optional) Enables stateful backup of redundant route processors for an IOS SLB virtual server. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate casa** command is not supported (because sessions are not persistent, and there is nothing to replicate). If you are using one Supervisor Engine with **replicate slave** configured, you might receive out-of-sync messages on the Supervisor.
Step 24	**sticky** {*duration*[**group** *group-id*] [**netmask** *netmask*] | **asn msid**[**group** *group-id*] | **gtp imsi**[**group** *group-id*] | **radius calling-station-id**| **radius framed-ip**[**group** *group-id*] | **radius username**[**msid-cisco**] [**group** *group-id*]}	(Optional) Specifies that connections from the same client use the same real server, as long as the interval between client connections does not exceed the specified duration. **Note** In VPN server load balancing, specify a *duration* of at least 15 seconds. GPRS load balancing and the Home Agent Director do not support this command.

	Command or Action	Purpose
	Example: `Router(config-slb-vserver)# sticky 60 group 10`	
Step 25	**synguard** *syn-count interval* **Example:** `Router(config-slb-vserver)# synguard 50`	(Optional) Specifies the rate of TCP SYNchronize sequence numbers (SYNs) managed by a virtual server in order to prevent a SYN flood denial-of-service attack. **Note** GPRS load balancing and the Home Agent Director do not support this command.
Step 26	**inservice** [**standby** *group-name*] [**active**] **Example:** `Router(config-slb-vserver)# inservice`	Enables the virtual server for use by IOS SLB.

How to Verify a Virtual Server

Perform the following optional task to verify a virtual server.

The following **show ip slb vservers** command verifies the configuration of the virtual servers PUBLIC_HTTP and RESTRICTED_HTTP:

```
Router# show ip slb vservers
slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
PUBLIC_HTTP      TCP   10.0.0.1:80           OPERATIONAL     0
RESTRICTED_HTTP  TCP   10.0.0.2:80           OPERATIONAL     0
Router#
```

How to Verify a Server Farm

Perform the following optional task to verify a server farm.

The following **show ip slb reals** command shows the status of server farms PUBLIC and RESTRICTED, the associated real servers, and their status:

```
Router# show ip slb real
real                    farm name        weight   state          conns
-------------------------------------------------------------------
10.1.1.1                 PUBLIC           8       OPERATIONAL      0
10.1.1.2                 PUBLIC           8       OPERATIONAL      0
10.1.1.3                 PUBLIC           8       OPERATIONAL      0
10.1.1.20                RESTRICTED       8       OPERATIONAL      0
10.1.1.21                RESTRICTED       8       OPERATIONAL      0
Router#
```

The following **show ip slb serverfarm**command displays the configuration and status of server farms PUBLIC and RESTRICTED:

```
Router# show ip slb serverfarm
server farm      predictor    nat   reals   bind id
-------------------------------------------------
PUBLIC           ROUNDROBIN   none  3       0
RESTRICTED       ROUNDROBIN   none  2       0
Router#
```

How to Verify Clients

Perform the following optional task to verify clients.

The following **show ip slb conns** command verifies the restricted client access and status:

```
Router# show ip slb conns
vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
RESTRICTED_HTTP TCP  10.4.4.0:80          10.1.1.20            CLOSING   none
Router#
```

The following **show ip slb conns** command shows detailed information about the restricted client access status:

```
Router# show ip slb conns client 10.4.4.0 detail
VSTEST_UDP, client = 10.4.4.0:80
  state = CLOSING, real = 10.1.1.20, nat = none
  v_ip = 10.0.0.2:80, TCP, service = NONE
  client_syns = 0, sticky = FALSE, flows attached = 0
Router#
```

How to Verify IOS SLB Connectivity

Perform the following optional task to verify IOS SLB connectivity.

To verify that the IOS SLB feature is installed and is operating correctly, ping the real servers from the IOS SLB switch, then ping the virtual servers from the clients.

The following **show ip slb stats** command shows detailed information about the IOS SLB network status:

```
Router# show ip slb stats
 Pkts via normal switching:  0
 Pkts via special switching: 6
 Pkts dropped:               0
 Connections Created:        1
 Connections Established:    1
 Connections Destroyed:      0
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         0
```

- Normal switching exists when IOS SLB packets are managed on normal IOS switching paths (CEF, fast switching, and process level switching).
- Special switching exists when IOS SLB packets are managed on hardware-assisted switching paths.

See "How to Monitor and Maintain the Cisco IOS SLB Feature" for additional commands used to verify IOS SLB networks and connections.

How to Configure Firewall Load Balancing

Perform the following tasks to configure a basic IOS SLB firewall load-balancing network.

IOS SLB firewall load balancing uses probes to detect and recover from failures. You must configure a probe on each real server in the firewall farm. Ping probes are recommended; see "How to Configure a Ping Probe" for more details. If a firewall does not allow ping probes to be forwarded, use HTTP probes instead. See "How to Configure an HTTP Probe" for more details. You can configure more than one probe, in any combination of supported types (DNS, HTTP, TCP, or ping), for each firewall in a firewall farm.

When you perform server load balancing and firewall load balancing together on a Cisco Catalyst 6500 switch, use the **mls ip slb wildcard search rp** command in global configuration mode to reduce the

probability of exceeding the capacity of the Telecommunications Access Method (TCAM) on the Policy Feature Card (PFC). See "How to Configure a Wildcard Search" for more details.

If IOS SLB experiences a high purge rate, the CPU might be impacted. If this problem occurs, use the **no** form of the **mls ip slb purge global** command in global configuration mode to disable purge throttling on TCP and UDP flow packets. See "How to Configure Protocol-Level Purging of MLS Entries" for more details.

This section describes the following IOS SLB firewall load-balancing configuration tasks. Required and optional tasks are indicated.

- How to Configure a Firewall Farm, page 13
- How to Verify a Firewall Farm, page 17
- How to Verify Firewall Connectivity, page 17

How to Configure a Firewall Farm

Perform the following required task to configure a firewall farm.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb firewallfarm** *firewall-farm*
4. **real** *ip-address*
5. **probe** *probe*
6. **weight** *setting*
7. **inservice**
8. **access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]
9. **predictor hash address** [**port**]
10. **purge connection**
11. **purge sticky**
12. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string*[*timeout*]]
13. **replicate interval** *interval*
14. **replicate slave**
15. **protocol tcp**
16. **delay** *duration*
17. **idle** *duration*
18. **maxconns** *maximum-number*
19. **sticky** *duration* [**netmask** *netmask*] [**source**| **destination**]
20. **protocol datagram**
21. **idle** *duration*
22. **maxconns** *maximum-number*
23. **sticky** *duration* [**netmask** *netmask*] [**source**| **destination**]
24. **inservice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb firewallfarm** *firewall-farm* **Example:** `Router(config)# ip slb firewallfarm FIRE1`	Adds a firewall farm definition to the IOS SLB configuration and enters firewall farm configuration mode.
Step 4	**real** *ip-address* **Example:** `Router(config-slb-fw)# real 10.1.1.1`	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.
Step 5	**probe** *probe* **Example:** `Router(config-slb-fw-real)# probe FireProbe`	Associates a probe with the firewall.
Step 6	**weight** *setting* **Example:** `Router(config-slb-fw-real)# weight 24`	(Optional) Specifies the firewall's workload capacity relative to other firewalls in the firewall farm.
Step 7	**inservice** **Example:** `Router(config-slb-fw-real)# inservice`	Enables the firewall for use by the firewall farm and by IOS SLB.
Step 8	**access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]	(Optional) Routes specific flows to a firewall farm.

	Command or Action	Purpose
	Example: `Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0`	
Step 9	**predictor hash address** [**port**] **Example:** `Router(config-slb-fw)# predictor hash address`	(Optional) Specifies whether the source and destination TCP or User Datagram Protocol (UDP) port numbers, in addition to the source and destination IP addresses, are to be used when selecting a firewall.
Step 10	**purge connection** **Example:** `Router(config-slb-fw)# purge connection`	(Optional) Enables IOS SLB firewall load balancing to send purge requests for connections.
Step 11	**purge sticky** **Example:** `Router(config-slb-fw)# purge sticky`	(Optional) Enables IOS SLB firewall load balancing to send purge requests for sticky connections when the sticky timer expires.
Step 12	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string*[*timeout*]] **Example:** `Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231`	(Optional) Configures a stateful backup of IOS SLB firewall load-balancing decision tables to a backup switch. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate casa** command is not supported (because sessions are not persistent, and there is nothing to replicate).
Step 13	**replicate interval** *interval* **Example:** `Router(config-slb-fw)# replicate interval 20`	(Optional) Sets the replication delivery interval for an IOS SLB firewall farm. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate interval** command is not supported (because sessions are not persistent, and there is nothing to replicate).
Step 14	**replicate slave** **Example:** `Router(config-slb-fw)# replicate slave`	(Optional) Enables stateful backup of redundant route processors for an IOS SLB firewall farm. **Note** The Home Agent Director does not support this command. If you specify the **service gtp** keyword on the **virtual** command, and you do not specify the **sticky** command with the **gtp imsi** keyword, the **replicate slave** command is not supported (because sessions are not persistent, and there is nothing to replicate). If you are using one Supervisor Engine with **replicate slave** configured, you might receive out-of-sync messages on the Supervisor.
Step 15	**protocol tcp**	(Optional) Enters firewall farm TCP protocol configuration mode.

	Command or Action	Purpose
	Example: `Router(config-slb-fw)# protocol tcp`	
Step 16	**delay** *duration* **Example:** `Router(config-slb-fw-tcp)# delay 30`	(Optional) In firewall farm TCP protocol configuration mode, specifies the time IOS SLB firewall load balancing maintains TCP connection context after a connection ends.
Step 17	**idle** *duration* **Example:** `Router(config-slb-fw-tcp)# idle 120`	(Optional) In firewall farm TCP protocol configuration mode, specifies the minimum time IOS SLB firewall load balancing maintains connection context in the absence of packet activity.
Step 18	**maxconns** *maximum-number* **Example:** `Router(config-slb-fw-tcp)# maxconns 1000`	(Optional) In firewall farm TCP protocol configuration mode, specifies the maximum number of active TCP connections allowed on the firewall farm at one time.
Step 19	**sticky** *duration* [**netmask** *netmask*] [**source**| **destination**] **Example:** `Router(config-slb-fw-tcp)# sticky 60`	(Optional) In firewall farm TCP protocol configuration mode, specifies that connections from the same IP address use the same firewall if either of the following conditions is met: • As long as any connection between the same pair of IP addresses exists (source and destination sticky). • For a period, defined by *duration* , after the last connection is destroyed.
Step 20	**protocol datagram** **Example:** `Router(config-slb-fw)# protocol datagram`	(Optional) Enters firewall farm datagram protocol configuration mode.
Step 21	**idle** *duration* **Example:** `Router(config-slb-fw-udp)# idle 120`	(Optional) In firewall farm datagram protocol configuration mode, specifies the minimum time IOS SLB firewall load balancing maintains connection context in the absence of packet activity.
Step 22	**maxconns** *maximum-number* **Example:** `Router(config-slb-fw-udp)# maxconns 1000`	(Optional) In firewall farm datagram protocol configuration mode, specifies the maximum number of active datagram connections allowed on the firewall farm at one time.
Step 23	**sticky** *duration* [**netmask** *netmask*] [**source**| **destination**]	(Optional) In firewall farm datagram protocol configuration mode, specifies that connections from the same IP address use the same firewall if either of the following conditions is met:

	Command or Action	Purpose
	Example: `Router(config-slb-fw-udp)# sticky 60`	• As long as any connection between the same pair of IP addresses exists (source and destination sticky). • For a period, defined by *duration* , after the last connection is destroyed.
Step 24	**inservice** **Example:** `Router(config-slb-fw)# inservice`	Enables the firewall farm for use by IOS SLB.

How to Verify a Firewall Farm

Perform the following optional task to verify a firewall farm.

The following **show ip slb reals** command shows the status of firewall farm FIRE1, the associated real servers, and the server status:

```
Router# show ip slb real
real                farm name        weight   state          conns
-------------------------------------------------------------------
10.1.1.2            FIRE1            8        OPERATIONAL    0
10.1.2.2            FIRE1            8        OPERATIONAL    0
```

The following **show ip slb firewallfarm**command shows the configuration and status of firewall farm FIRE1:

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-------------------------------------------------
FIRE1            IPADDR      INSERVICE     2
```

How to Verify Firewall Connectivity

Perform the following optional task to verify firewall connectivity.

To verify that IOS SLB firewall load balancing is configured and is operating correctly, perform the following steps:

SUMMARY STEPS

1. Ping the external real servers (the ones outside the firewall) from the IOS SLB firewall load-balancing switch.
2. Ping the internal real servers (the ones inside the firewall) from the clients.
3. Use the **show ip slb stats** command to show information about the IOS SLB firewall load-balancing network status:
4. Use the **show ip slb real detail**command to show information about the IOS SLB firewall load-balancing real server status:
5. Use the **show ip slb conns**command to show information about the active IOS SLB firewall load-balancing connections:

DETAILED STEPS

Step 1 Ping the external real servers (the ones outside the firewall) from the IOS SLB firewall load-balancing switch.

Step 2 Ping the internal real servers (the ones inside the firewall) from the clients.

Step 3 Use the **show ip slb stats** command to show information about the IOS SLB firewall load-balancing network status:

Example:

```
Router# show ip slb stats
 Pkts via normal switching:  0
 Pkts via special switching: 0
 Pkts dropped:               0
 Connections Created:        1911871
 Connections Established:    1967754
 Connections Destroyed:      1313251
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         59752
 Connection Flowcache Purges:1776582
 Failed Connection Allocs:   17945
 Failed Real Assignments:    0
```

- Normal switching exists when IOS SLB packets are managed on normal IOS switching paths (CEF, fast switching, and process level switching).
- Special switching exists when IOS SLB packets are managed on hardware-assisted switching paths.

Step 4 Use the **show ip slb real detail**command to show information about the IOS SLB firewall load-balancing real server status:

Example:

```
Router# show ip slb reals detail
172.16.88.5, SF1, state = OPERATIONAL, type = server
  ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

Step 5 Use the **show ip slb conns**command to show information about the active IOS SLB firewall load-balancing connections:

Example:

```
Router# show ip slb conns
vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
```

See "How to Monitor and Maintain the Cisco IOS SLB Feature" for additional commands used to verify IOS SLB networks and connections.

How to Configure a Probe

The following sections describe how to configure and verify probes. By default, no probes are configured in IOS SLB.

IOS SLB uses probes to verify connectivity and detect failures. For a detailed description of each type of probe, see the “Probes” section.

Perform the following task to configure a probe. Required and optional tasks are indicated.

- How to Configure a Custom UDP Probe, page 19
- How to Configure a DNS Probe, page 21
- How to Configure an HTTP Probe, page 22
- How to Configure a Ping Probe, page 24
- How to Configure a TCP Probe, page 25
- How to Configure a WSP Probe, page 26
- How to Associate a Probe, page 27
- How to Verify a Probe, page 28

How to Configure a Custom UDP Probe

Perform the following task to configure a custom User Datagram Protocol (UDP) probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **custom udp**
4. **address** [*ip-address*] [**routed**]
5. **faildetect** *number-of-probes*
6. **interval** *seconds*
7. **port** *port*
8. **request data** {*start-byte* | **continue**} *hex-data-string*
9. **response** *clause-number* **data** *start-byte hex-data-string*
10. **timeout** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Router# configure terminal`	
Step 3	**ip slb probe** *probe* **custom udp** **Example:** `Router(config)# ip slb probe PROBE6 custom udp`	Configures the IOS SLB probe name and enters custom User Datagram Protocol (UDP) probe configuration mode.
Step 4	**address** [*ip-address*] [**routed**] **Example:** `Router(config-slb-probe)# address 10.1.1.1`	(Optional) Configures an IP address to which to send the custom UDP probe.
Step 5	**faildetect** *number-of-probes* **Example:** `Router(config-slb-probe)# faildetect 16`	(Optional) Specifies the number of consecutive unacknowledged custom UDP probes that constitute failure of the real server.
Step 6	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 11`	(Optional) Configures the custom UDP probe transmit timers.
Step 7	**port** *port* **Example:** `Router(config-slb-probe)# port 8`	Configures the port to which the custom UDP probe is to connect.
Step 8	**request data** {*start-byte* | **continue**} *hex-data-string* **Example:** `Router(config-slb-probe)# request data 0 05 04 00 77 18 2A D6 CD 0A AD 53 4D F1 29 29 CF C1 96 59 CB`	Defines the payload of the UDP request packet to be sent by a custom UDP probe.
Step 9	**response** *clause-number* **data** *start-byte hex-data-string* **Example:** `Router(config-slb-probe)# response 2 data 44 DD DD`	Defines the data string to match against custom UDP probe response packets.
Step 10	**timeout** *seconds* **Example:** `Router(config-slb-probe)# timeout 20`	(Optional) Sets a timeout for custom UDP probes.

How to Configure a DNS Probe

Perform the following task to configure a Domain Name System (DNS) probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **dns**
4. **address** [*ip-address* [**routed**]]
5. **faildetect** *number-of-probes*
6. **interval** *seconds*
7. **lookup** *ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb probe** *probe* **dns** **Example:** `Router(config)# ip slb probe PROBE4 dns`	Configures the IOS SLB probe name and enters Domain Name System (DNS) probe configuration mode.
Step 4	**address** [*ip-address* [**routed**]] **Example:** `Router(config-slb-probe)# address 10.1.10.1`	(Optional) Configures an IP address to which to send the DNS probe.
Step 5	**faildetect** *number-of-probes* **Example:** `Router(config-slb-probe)# faildetect 16`	(Optional) Specifies the number of consecutive unacknowledged DNS probes that constitute failure of the real server or firewall.
Step 6	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 11`	(Optional) Configures the DNS probe transmit timers.

	Command or Action	Purpose
Step 7	**lookup** *ip-address* **Example:** `Router(config-slb-probe)# lookup 10.1.10.1`	(Optional) Configures an IP address of a real server that a DNS server should supply in response to a domain name resolve request.

How to Configure an HTTP Probe

Perform the following task to configure an HTTP probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **http**
4. **address** [*ip-address* [**routed**]]
5. **credentials** {*username* [*password*]}
6. **expect** [**status** *status-code*] [**regex** *expression*]
7. **header** *field-name* [*field-value*]
8. **interval** *seconds*
9. **port** *port*
10. **request** [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]
11. Configure a route to the virtual server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb probe** *probe* **http** **Example:** `Router(config)# ip slb probe PROBE2 http`	Configures the IOS SLB probe name and enters HTTP probe configuration mode.
Step 4	**address** [*ip-address* [**routed**]]	(Optional) Configures an IP address to which to send the HTTP probe.

	Command or Action	Purpose
	Example: `Router(config-slb-probe)# address 10.1.10.1`	
Step 5	**credentials** {*username* [*password*]} **Example:** `Router(config-slb-probe)# credentials Username1 password`	(Optional) Configures header values for the HTTP probe.
Step 6	**expect** [**status** *status-code*] [**regex** *expression*] **Example:** `Router(config-slb-probe)# expect status 401 regex Copyright`	(Optional) Configures the expected HTTP status code or regular expression.
Step 7	**header** *field-name* [*field-value*] **Example:** `Router(config-slb-probe)# header HeaderName HeaderValue`	(Optional) Configures header values for the HTTP probe.
Step 8	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 11`	(Optional) Configures the HTTP probe transmit timers.
Step 9	**port** *port* **Example:** `Router(config-slb-probe)# port 8`	(Optional) Configures the port to which the HTTP probe is to connect.
Step 10	**request** [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*] **Example:** `Router(config-slb-probe)# request method post url /probe.cgi?all`	(Optional) Configures the URL path to request from the server, and the method used to perform the request to the server.
Step 11	Configure a route to the virtual server.	HTTP probes require a route to the virtual server. The route is not used, but it must exist to enable the socket code to verify that the destination can be reached, which in turn is essential for HTTP probes to function correctly. The route can be either: • Host route--Advertised by the virtual server • Default route--Specified using the **ip route 0.0.0.0 0.0.0.0**command, for example

How to Configure a Ping Probe

Perform the following task to configure a ping probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **ping**
4. **address** [*ip-address* [**routed**]]
5. **faildetect** *number-of-pings*
6. **interval** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb probe** *probe* **ping** **Example:** `Router(config)# ip slb probe PROBE1 ping`	Configures the IOS SLB probe name and enters ping probe configuration mode.
Step 4	**address** [*ip-address* [**routed**]] **Example:** `Router(config-slb-probe)# address 10.1.10.1`	(Optional) Configures an IP address to which to send the ping probe.
Step 5	**faildetect** *number-of-pings* **Example:** `Router(config-slb-probe)# faildetect 16`	(Optional) Specifies the number of consecutive unacknowledged pings that constitute failure of the real server or firewall.
Step 6	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 11`	(Optional) Configures the ping probe transmit timers.

How to Configure a TCP Probe

Perform the following task to configure a TCP probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **tcp**
4. **address** [*ip-address* [**routed**]]
5. **interval** *seconds*
6. **port** *port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb probe** *probe* **tcp** **Example:** `Router(config)# ip slb probe PROBE5 tcp`	Configures the IOS SLB probe name and enters TCP probe configuration mode.
Step 4	**address** [*ip-address* [**routed**]] **Example:** `Router(config-slb-probe)# address 10.1.10.1`	(Optional) Configures an IP address to which to send the TCP probe.
Step 5	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 5`	(Optional) Configures the TCP probe transmit timers.
Step 6	**port** *port* **Example:** `Router(config-slb-probe)# port 8`	Configures the port to which the TCP probe is to connect.

How to Configure a WSP Probe

Perform the following task to configure a Wireless Session Protocol (WSP) probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **wsp**
4. **address** [*ip-address* [**routed**]]
5. **interval** *seconds*
6. **url** [*path*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb probe** *probe* **wsp** **Example:** `Router(config)# ip slb probe PROBE3 wsp`	Configures the IOS SLB probe name and enters Wireless Session Protocol (WSP) probe configuration mode.
Step 4	**address** [*ip-address* [**routed**]] **Example:** `Router(config-slb-probe)# address 10.1.10.1`	(Optional) Configures an IP address to which to send the WSP probe.
Step 5	**interval** *seconds* **Example:** `Router(config-slb-probe)# interval 11`	(Optional) Configures the WSP probe transmit timers.
Step 6	**url** [*path*] **Example:** `Router(config-slb-probe)# url http://localhost/test.txt`	(Optional) Configures the WSP probe URL path.

How to Associate a Probe

Perform the following task to associate a probe with a real server or firewall.

After configuring a probe, you must associate the probe with a real server or firewall using the **probe** command. See "How to Configure a Server Farm and a Real Server" and "How to Configure Firewall Load Balancing" for more details.

Note You cannot associate a WSP probe with a firewall.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ip slb firewallfarm** *firewall-farm*
   -
   - **ip slb serverfarm** *server-farm*
4. Do one of the following:
   - **probe** *probe*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **ip slb firewallfarm** *firewall-farm* • • **ip slb serverfarm** *server-farm* **Example:** `Router(config)# ip slb serverfarm PUBLIC`	Identifies a firewall farm and enters firewall farm configuration mode. or Identifies a server farm and enters SLB server farm configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# ip slb firewallfarm FIRE1`	

Step 4	Do one of the following:
	• **probe** *probe*
	Example:
	`Router(config-slb-sfarm)# probe PROBE1`
	Example:
	`Router(config-slb-fw-real)# probe FireProbe`
		Associates a probe with a firewall farm or a server farm.

How to Verify a Probe

Perform the following optional task to verify a probe.

To verify that a probe is configured correctly, use the **show ip slb probe**command:

```
Router# show ip slb probe
Server:Port            State        Outages  Current  Cumulative
---------------------------------------------------------------
10.1.1.1:80            OPERATIONAL        0  never    00:00:00
10.1.1.2:80            OPERATIONAL        0  never    00:00:00
10.1.1.3:80            OPERATIONAL        0  never    00:00:00
```

How to Configure DFP

Perform the following task to configure IOS SLB as a Dynamic Feedback Protocol (DFP) manager, and to identify a DFP agent with which IOS SLB can initiate connections.

You can define IOS SLB as a DFP manager, as a DFP agent for another DFP manager, or as both at the same time. Depending on your network configuration, you might enter the commands for configuring IOS SLB as a DFP manager and the commands for configuring IOS SLB as a DFP agent on the same device or on different devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb dfp** [**password**[[*encrypt*] *secret-string* [*timeout*]]
4. **agent** *ip-address port* [*timeout*[*retry-count* [*retry-interval*]]]
5. Configure IOS SLB as a DFP agent.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb dfp** [**password**[[*encrypt*] *secret-string* [*timeout*]] **Example:** `Router(config)# ip slb dfp password Password1 360`	Configures Dynamic Feedback Protocol (DFP), supplies an optional password, and enters DFP configuration mode.
Step 4	**agent** *ip-address port* [*timeout*[*retry-count* [*retry-interval*]]] **Example:** `Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10`	Identifies a DFP agent to which IOS SLB can connect.
Step 5	Configure IOS SLB as a DFP agent.	To configure IOS SLB as a DFP agent, refer to the *DFP Agent Subsystem* feature document for Cisco IOS Release 12.2(18)SXB.

GPRS Load Balancing Configuration Task List

Perform the following tasks to configure general packet radio service (GPRS) load balancing.

SUMMARY STEPS

1. Configure a server farm and a real server.
2. Configure a virtual server.
3. Configure the virtual IP address as a loopback on each of the GGSNs in the servers.
4. Route each GGSN to each associated SGSN.
5. Route each SGSN to the virtual templates on each associated Cisco GGSN, and to the GPRS load-balancing virtual server.
6. Configure a GSN idle timer.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server".

	Command or Action	Purpose
		When you configure the server farm and real server for GPRS load balancing, keep the following considerations in mind: • If GTP cause code inspection: ◦ Is not enabled--Accept the default setting (the weighted round robin algorithm) for the **predictor** command. ◦ Is enabled--Specify either the weighted round robin (**roundrobin**) or the weighted least connections (**leastconns**) algorithm. • Specify the IP addresses (virtual template addresses for Cisco GGSNs) of the real servers performing the GGSN function, using the **real** command. • Specify a reassign threshold less than the SGSN's N3-REQUESTS counter value using the **reassign** command. • To enable dual-stack support for GTP load balancing: ◦ Specify the real server's IPv6 address using the **real**command.
Step 2	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the **virtual** command, keep the following considerations in mind: • Specify a virtual GGSN IP address as the virtual server, and specify the **udp** keyword option. • To load-balance GTP v1 and GTP v2 sessions, specify port number 2123, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports). • To load-balance GTP v0 sessions, specify port number 3386, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any** to configure an all-port virtual server. • To enable GPRS load balancing: ◦ *Without* GTP cause code inspection--Specify the **service gtp**keyword option. In GPRS load balancing *without* GTP cause code inspection enabled, when you configure the idle timer using the **idle** command, specify an idle timer greater than the longest possible interval between PDP context requests on the SGSN. • ◦ *With* GTP cause code inspection--Specify the **service gtp-inspect**keyword option. • To enable dual-stack support for GTP load balancing: ◦ Specify the virtual server's IPv6 address and optional IPv6 prefix, using the **virtual** command. ◦ Associate the primary IPv6 server farm and optional backup IPv6 server farm with the virtual server, using the **serverfarm**command. ◦ Remove the **client** command from the configuration.
Step 3	Configure the virtual IP address as a loopback on each of the GGSNs in the servers.	(Required for dispatched mode) This step is required only if you are using dispatched mode *without* GTP cause code inspection enabled. Refer to the *Cisco IOS Interface Configuration Guide* "Configuring Virtual Interfaces" section for more information.

	Command or Action	Purpose
Step 4	Route each GGSN to each associated SGSN.	The route can be static or dynamic, but the GGSN needs to be able to reach the SGSN. Refer to the *Cisco IOS Mobile Wireless Configuration Guide* “Configuring Network Access to the GGSN” section for more details.
Step 5	Route each SGSN to the virtual templates on each associated Cisco GGSN, and to the GPRS load-balancing virtual server.	(Required) Refer to the configuration guide for your SGSN for more details.
Step 6	Configure a GSN idle timer.	(Optional) This step is applicable only if GTP cause code inspection is enabled. See "How to Configure a GSN Idle Timer" for more information.

- How to Configure a GSN Idle Timer, page 31

How to Configure a GSN Idle Timer

Perform this task to configure a GPRS support node (GSN) idle timer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb timers gtp gsn** *duration*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb timers gtp gsn** *duration* **Example:** `Router(config)# ip slb timers gtp gsn 45`	Change the amount of time IOS SLB maintains sessions to and from an idle gateway GPRS support node (GGSN) or serving GPRS support node (SGSN).

GGSN-IOS SLB Messaging Task List

Perform this task to configure GGSN-IOS SLB messaging.

SUMMARY STEPS

1. Configure the GGSN to support GGSN-IOS SLB messaging.
2. Configure a server farm and a real server.
3. Configure a virtual server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure the GGSN to support GGSN-IOS SLB messaging.	When you configure GGSN-IOS SLB messaging support, configure all IOS SLB virtual servers that share the same GGSN to use the same NAT mode, either dispatched mode or directed mode, using the **gprs slb mode**command. The virtual servers cannot use a mix of dispatched mode and directed mode, because you can configure only one NAT mode on a given GGSN. For more information, refer to the *Cisco IOS Mobile Wireless Configuration Guide* for GGSN Release 5.0 for Cisco IOS Release 12.3(2)XU or later.
Step 2	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for GGSN-IOS SLB messaging, to prevent IOS SLB from failing the current real server when reassigning the session to a new real server, disable automatic server failure detection by specifying the **no faildetect inband** command.
Step 3	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the virtual server for GGSN-IOS SLB messaging, specify the **gtp notification cac**command to limit the number of times IOS SLB can reassign a session to a new real server.

How to Configure GPRS Load Balancing Maps

Perform this task to configure GPRS load balancing maps.

GPRS load balancing maps enable IOS SLB to categorize and route user traffic based on access point names (APNs). To enable maps for GPRS load balancing, you must define a GPRS Tunneling Protocol (GTP) map, then associate the map with a server farm.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb map** *map-id* **gtp** | **radius**}
4. **apn** *string*
5. **exit**
6. **ip slb vserver** *virtual-server*
7. **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*]
8. **serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb map** *map-id* **gtp** | **radius**} **Example:** `Router(config)# ip slb map 1 radius`	Configures an IOS SLB GTP map and enters SLB GTP map configuration mode.
Step 4	**apn** *string* **Example:** `Router(config-slb-map-gtp)# apn abc`	Configures an ASCII regular expression string to be matched against the access point name (APN) for general packet radio service (GPRS) load balancing.
Step 5	**exit** **Example:** `Router(config-slb-map-gtp)# exit`	Exits SLB GTP map configuration mode.
Step 6	**ip slb vserver** *virtual-server* **Example:** `Router(config)# ip slb vserver GGSN_SERVER`	Identifies a virtual server and enters virtual server configuration mode.
Step 7	**virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*] **Example:** `Router(config-slb-vserver)# virtual 10.10.10.10 udp 0 service gtp`	Specifies the virtual server IP address, type of connection, and optional TCP or User Datagram Protocol (UDP) port number, Internet Key Exchange (IKE) or Wireless Session Protocol (WSP) setting, and service coupling. **Note** For GPRS load balancing: • ◦ Specify a virtual GGSN IP address as the virtual server, and specify the **udp** keyword option. ◦ To load-balance GTP v1 and GTP v2 sessions, specify port number 2123, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports).

	Command or Action	Purpose
		◦ To load-balance GTP v0 sessions, specify port number 3386, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number 0 or **any**to configure an all-port virtual server. ◦ To enable GPRS load balancing *without* GTP cause code inspection, specify the **service gtp**keyword option. ◦ To enable GPRS load balancing *with* GTP cause code inspection, specify the **service gtp-inspect**keyword option. ◦ For dual-stack support for GTP load balancing, specify the virtual server's IPv4 and IPv6 addresses and optional IPv6 prefix.
Step 8	**serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] **Example:** `Router(config-slb-vserver)# serverfarm farm1 backup farm2 map 1 priority 3`	Associates a GTP map with a server farm. Associates a real server farm with a virtual server, and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm. **Note**For GPRS load balancing, if a real server is defined in two or more server farms, each server farm must be associated with a different virtual server. You can associate more than one server farm with a virtual server by configuring more than one **serverfarm** command, each with a unique map ID and a unique priority. (That is, each map ID and each map priority must be unique across all server farms associated with the virtual server.) If you are using GTP maps, and you have configured a real server in more than one server farm, you must associate a different virtual server with each server farm.

How to Configure KAL-AP Agent Support

Perform this task to configure KeepAlive Application Protocol (KAL-AP) agent support.

KAL-AP agent support enables IOS SLB to perform load balancing in a global server load balancing (GSLB) environment.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb capp udp**
4. **peer** [*ip-address*] **port** *port*
5. **peer** [*ip-address*] **secret** [*encrypt*] *secret-string*
6. **exit**
7. **ip slb serverfarm** *server-farm*
8. **kal-ap domain** *tag*
9. **farm-weight** *setting*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb capp udp** **Example:** `Router(config)# ip slb capp udp`	Enables the KAL-AP agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.
Step 4	**peer** [*ip-address*] **port** *port* **Example:** `Router(config-slb-capp)# peer port 6000`	(Optional) Specifies the port to which the KAL-AP agent is to connect.
Step 5	**peer** [*ip-address*] **secret** [*encrypt*] *secret-string* **Example:** `Router(config-slb-capp)# peer secret SECRET_STRING`	(Optional) Enables Message Digest Algorithm Version 5 (MD5) authentication for the KAL-AP agent.
Step 6	**exit** **Example:** `Router(config-slb-map-gtp)# exit`	Exits SLB CAPP configuration mode.
Step 7	**ip slb serverfarm** *server-farm* **Example:** `Router(config)# ip slb serverfarm PUBLIC`	Identifies a server farm and enters SLB server farm configuration mode.
Step 8	**kal-ap domain** *tag* **Example:** `Router(config-slb-sfarm)# kal-ap domain chicago-com`	(Optional) Enables the KAL-AP agent to look for a domain tag when reporting the load for a virtual server.
Step 9	**farm-weight** *setting*	(Optional) Specifies a weight to be used by the KAL-AP agent when calculating the load value for a server farm.

	Command or Action	Purpose
	Example: `Router(config-slb-sfarm)# farm-weight 16`	

RADIUS Load Balancing Configuration Task List

Perform this task to configure RADIUS load balancing.

SUMMARY STEPS

1. Configure a server farm and a real server.
2. Configure a virtual server.
3. Configure a virtual server. (continued)
4. Enable IOS SLB to inspect packets for RADIUS framed-IP sticky routing.
5. Configure RADIUS load balancing maps.
6. Configure RADIUS load balancing accelerated data plane forwarding.
7. Increase the number of available MLS entries.
8. Configure a probe.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for RADIUS load balancing, keep the following considerations in mind: • Accept the default setting (the weighted round robin algorithm) for the **predictor** command. • (Optional) To enable session-based failure detection, specify a value of 1 for the **numclients** keyword on the **faildetect numconns**command. • (Optional) To specify the maximum number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server, use the **maxclients** command.
Step 2	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the virtual server for RADIUS load balancing, keep the following considerations in mind: • Specify the **service radius**keyword option, using the **virtual** command. • (Optional) To enable framed-IP routing to inspect the ingress interface, specify the **access***interface* **route framed-ip**command. If you configure the **access***interface* **route framed-ip**command, you must also configure the **virtual** command with the **service radius**keywords specified. • (Optional) To change the amount of time IOS SLB waits for an ACCT-START message from a new mobile IP foreign agent in the event of a foreign agent hand-off, configure a **hand-off radius**command.

	Command or Action	Purpose
		• (Optional) To set a duration for RADIUS entries in the IOS SLB session database, configure an **idle** command with the **radius request** keywords specified. • (Optional) To set a duration for entries in the IOS SLB RADIUS framed-IP sticky database, configure an **idle** command with the **radius framed-ip** keywords specified.
Step 3	Configure a virtual server. (continued)	• (Optional) To enable IOS SLB to create the IOS SLB RADIUS framed-IP sticky database and direct RADIUS requests and non-RADIUS flows from a subscriber to the same service gateway, specify the **sticky**command with the **radius framed-ip**keywords. If you configure the **sticky radius framed-ip**command, you must also configure the **virtual** command with the **service radius**keywords specified. • (Optional) To enable IOS SLB to purge entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting On or Off message, specify the **purge radius framed-ip acct on-off virtual server**configuration command. To prevent IOS SLB from purging entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting On or Off message, specify the **no purge radius framed-ip acct on-off virtual server**configuration command. • (Optional) To enable IOS SLB to purge entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting-Stop message, specify the **purge radius framed-ip acct stop virtual server**configuration command. To prevent IOS SLB from purging entries in the IOS SLB RADIUS framed-IP sticky database upon receipt of an Accounting-Stop message, specify the **no purge radius framed-ip acct stop virtual server**configuration command. • (Optional--For CDMA2000 networks only) To enable IOS SLB to create the IOS SLB RADIUS calling-station-ID sticky database and direct RADIUS requests from a subscriber to the same service gateway based on the calling station ID, specify the **sticky**command with the **radius calling-station-id**keywords. To enable IOS SLB to create the IOS SLB RADIUS username sticky database and direct RADIUS requests from a subscriber to the same service gateway based on the username, specify the **sticky**command with the **radius username**keywords. If you configure the **sticky radius calling-station-id**command or the **sticky radius username**command, you must also configure the **virtual** command with the **service radius**keywords specified, and you must configure the **sticky radius framed-ip**command. You cannot configure both the **sticky radius calling-station-id** command and the **sticky radius username** command on the same virtual server. • (Optional--For RADIUS load balancing accelerated data plane forwarding only) To configure a VSA correlation group for an authentication virtual server, and to specify whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames, configure the **radius inject auth** command. To configure a timer for VSA correlation for an authentication virtual server, configure the **radius inject auth timer**command. To buffer VSAs for VSA correlation for an authentication virtual server, configure the **radius inject auth vsa**command.

	Command or Action	Purpose
		To configure a VSA correlation group for an accounting virtual server, and to enable Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation, configure the **radius inject acct** command.
Step 4	Enable IOS SLB to inspect packets for RADIUS framed-IP sticky routing.	(Optional) See "How to Enable IOS SLB to Inspect Packets for RADIUS Framed-IP Sticky Routing".
Step 5	Configure RADIUS load balancing maps.	(Optional) See "How to Configure RADIUS Load Balancing Maps".
Step 6	Configure RADIUS load balancing accelerated data plane forwarding.	(Optional) See "How to Configure RADIUS Load Balancing Accelerated Data Plane Forwarding".
Step 7	Increase the number of available MLS entries.	(Optional) If you are running IOS SLB in dispatched mode on a Cisco Catalyst 6500 series switch with Cisco Supervisor Engine 2, you can improve performance by configuring the **no mls netflow** command. This command increases the number of MLS entries available for hardware switching of end-user flows. **Note** If you are using IOS features that use the hardware NetFlow table, such as microflow QoS, reflexive ACLs, TCP intercept, or Web Cache Redirect, do not configure the **no mls netflow** command. For more information about configuring MLS NetFlow, refer to the *Cisco Catalyst 6000 Family IOS Software Configuration Guide* .
Step 8	Configure a probe.	See "How to Configure a Probe". To verify the health of the server, configure a ping probe.

- How to Enable IOS SLB to Inspect Packets for RADIUS Framed-IP Sticky Routing, page 38
- How to Configure RADIUS Load Balancing Maps, page 39
- How to Configure RADIUS Load Balancing Accelerated Data Plane Forwarding, page 41

How to Enable IOS SLB to Inspect Packets for RADIUS Framed-IP Sticky Routing

You can enable IOS SLB to inspect packets whose source IP addresses match a configured IP address and subnet mask. If the source IP address of an inspected packet matches an entry in the IOS SLB RADIUS framed-IP sticky database, IOS SLB uses that entry to route the packet. Otherwise, IOS routes the packet.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb route framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb route framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall** **Example:** `Router(config)# ip slb route 10.10.10.1 255.255.255.255 framed-ip`	Enables IOS SLB to route packets using the RADIUS framed-IP sticky database, or to route packets from one firewall real server back through another firewall real server.

How to Configure RADIUS Load Balancing Maps

RADIUS load balancing maps enable IOS SLB to categorize and route user traffic based on RADIUS calling station IDs and usernames. To enable maps for RADIUS load balancing, you must define a RADIUS map, then associate the map with a server farm.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb map** *map-id* **radius**
4. **calling-station-id** *string*
5. **username** *string*
6. **exit**
7. **ip slb vserver** *virtual-server*
8. **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*]
9. **serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. If prompted, enter your password.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb map** *map-id* **radius** **Example:** `Router(config)# ip slb map 1 radius`	Configures an IOS SLB RADIUS map and enters SLB RADIUS map configuration mode.
Step 4	**calling-station-id** *string* **Example:** `Router(config-slb-radius-map)# calling-station-id .919*`	Configures an ASCII regular expression string to be matched against the calling station ID attribute for RADIUS load balancing.
Step 5	**username** *string* **Example:** `Router(config-slb-map-radius)# )# username ...?525*`	Configures an ASCII regular expression string to be matched against the username attribute for RADIUS load balancing.
Step 6	**exit** **Example:** `Router(config-slb-map-gtp)# exit`	Exits SLB RADIUS map configuration mode.
Step 7	**ip slb vserver** *virtual-server* **Example:** `Router(config)# ip slb vserver GGSN_SERVER`	Identifies a virtual server and enters virtual server configuration mode.
Step 8	**virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*] **Example:** `Router(config-slb-vserver)# virtual 10.0.0.1 udp 0 service radius`	Specifies the virtual server IP address, type of connection, and optional TCP or User Datagram Protocol (UDP) port number, Internet Key Exchange (IKE) or Wireless Session Protocol (WSP) setting, and service coupling. **Note** For RADIUS load balancing, specify the **service radius** keyword option.
Step 9	**serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-*	Associates a RADIUS map with a server farm. Associates a real server farm with a virtual server, and optionally configures a backup server

	Command or Action	Purpose
	farm[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] **Example:** `Router(config-slb-vserver)# serverfarm SF1 backup SF2 map 1 priority 1`	farm and specifies that sticky connections are to be used in the backup server farm. **Note**RADIUS load balancing does not support the **sticky**keyword. You can associate more than one server farm with a virtual server by configuring more than one **serverfarm** command, each with a unique map ID and a unique priority. (That is, each map ID and each map priority must be unique across all server farms associated with the virtual server.)

How to Configure RADIUS Load Balancing Accelerated Data Plane Forwarding

Perform this task to configure RADIUS load balancing accelerated data plane forwarding.

RADIUS load balancing accelerated data plane forwarding, also known as Turbo RADIUS load balancing, is a high-performance solution that uses basic policy-based routing (PBR) route maps to manage subscriber data-plane traffic in a Cisco Content Services Gateway (CSG) environment.

Turbo RADIUS load balancing requires a server farm configured with **predictor route-map** on the accounting virtual server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **predictor** [**roundrobin**| **leastconns**| **route-map** *mapname*]
5. **exit**
6. **ip slb vserver** *virtual-server*
7. **virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*]
8. **serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]
9. **radius acct local-ack key** [*encrypt*] *secret-string*
10. **radius inject auth** *group-number* {**calling-station-id**| **username**}
11. **radius inject auth timer** *seconds*
12. **radius inject auth vsa** *vendor-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode. If prompted, enter your password.

	Command or Action	Purpose
	Example: `Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb serverfarm** *server-farm* **Example:** `Router(config)# ip slb serverfarm PUBLIC`	Identifies a server farm and enters SLB server farm configuration mode.
Step 4	**predictor** [**roundrobin**| **leastconns**| **route-map** *mapname*] **Example:** `Router(config-slb-sfarm)# predictor route-map map1`	(Optional) Specifies the algorithm to be used to determine how a real server is selected. Turbo RADIUS load balancing requires the **route-map** keyword and *mapname* argument. When you specify the **predictor route-map** command, no further commands in SLB server farm configuration mode or real server configuration mode are allowed.
Step 5	**exit** **Example:** `Router(config-slb-sfarm)# exit`	Exits SLB server farm configuration mode.
Step 6	**ip slb vserver** *virtual-server* **Example:** `Router(config)# ip slb vserver RADIUS_AUTH`	Identifies a virtual server and enters virtual server configuration mode.
Step 7	**virtual** *ipv4-address* [*ipv4-netmask*[**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp**| **udp**} [*port*| **any**] [**service** *service*] **Example:** `Router(config-slb-vserver)# virtual 10.10.10.10 udp 1813 service radius`	Specifies the virtual server IP address, type of connection, and optional TCP or User Datagram Protocol (UDP) port number, Internet Key Exchange (IKE) or Wireless Session Protocol (WSP) setting, and service coupling and enters SLB virtual server configuration mode. **Note** For RADIUS load balancing, specify the **service radius** keyword option.
Step 8	**serverfarm** *primary-farm* [**backup** *backup-farm*[**sticky**]] [**ipv6-primary** *ipv6-primary-farm*[**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]	Associates a RADIUS map with a server farm. Associates a real server farm with a virtual server, and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm. **Note** RADIUS load balancing does not support the **sticky** keyword.

	Command or Action	Purpose
	Example: `Router(config-slb-vserver)# serverfarm AAAFARM`	You can associate more than one server farm with a virtual server by configuring more than one **serverfarm** command, each with a unique map ID and a unique priority. (That is, each map ID and each map priority must be unique across all server farms associated with the virtual server.)
Step 9	**radius acct local-ack key** [*encrypt*] *secret-string* **Example:** `Router(config-slb-vserver)# radius acct local-ack key SECRET_PASSWORD`	(Optional) Configures VSA correlation and enables a RADIUS virtual server to acknowledge RADIUS accounting messages **Note** If vendor-specific attribute (VSA) correlation is configured, and if the Cisco VSA is buffered, then the Cisco VSA is injected into the RADIUS Accounting-Start packet. Turbo RADIUS load balancing does not require VSA correlation. This command is valid only for VSA correlation accounting virtual servers.
Step 10	**radius inject auth** *group-number* {**calling-station-id**| **username**} **Example:** `Router(config-slb-vserver)# radius inject auth 1 calling-station-id`	(Optional) Configures a VSA correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and specifies whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames. For a given authentication virtual server, you can configure one **radius inject auth***group-number* **calling-station-id** command or one **radius inject auth***group-number* **username**command, but not both. This command is valid only for VSA correlation authentication virtual servers.
Step 11	**radius inject auth timer** *seconds* **Example:** `Router(config-slb-vserver)# radius inject auth timer 45`	(Optional) Configures a timer for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server. This command is valid only for VSA correlation authentication virtual servers.
Step 12	**radius inject auth vsa** *vendor-id* **Example:** `Router(config-slb-vserver)# radius inject auth vsa vendor1`	(Optional) Buffers VSAs for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server. This command is valid only for VSA correlation authentication virtual servers.

Exchange Director for mSEF Configuration Task List

Perform this task to configure Exchange Director for mobile Service Exchange Framework (mSEF).

- RADIUS Configuration for the Exchange Director, page 43
- Firewall Configuration for the Exchange Director, page 45

RADIUS Configuration for the Exchange Director

Perform this task to configure RADIUS load balancing for the Exchange Director.

SUMMARY STEPS

1. Configure a server farm and a real server.
2. Configure a virtual server.
3. Configure a virtual server. (continued)
4. Enable IOS SLB to inspect packets for RADIUS framed-IP sticky routing.
5. Configure RADIUS load balancing maps.
6. Increase the number of available MLS entries.
7. Configure a probe.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for RADIUS for the Exchange Director, keep the following considerations in mind: • (Optional) Specify a value of 1 for the **numclients** keyword on the **faildetect numconns**command, if you want to enable session-based failure detection. • (Optional) To specify the maximum number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server, use the **maxclients** command.
Step 2	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the virtual server for RADIUS for the Exchange Director, keep the following considerations in mind: • Specify the **service radius**keyword option, using the **virtual** command. • (Optional) To enable framed-IP routing to inspect the ingress interface, specify the **access***interface* **route framed-ip**command. If you configure the **access***interface* **route framed-ip**command, you must also configure the **virtual** command with the **service radius**keywords specified. • (Optional) To change the amount of time IOS SLB waits for an ACCT-START message from a new Mobile IP foreign agent in the event of a foreign agent hand-off, configure a **hand-off radius**command. • (Optional) To set a duration for RADIUS entries in the IOS SLB session database, configure an **idle** command with the **radius request** keywords specified. • (Optional) To set a duration for entries in the IOS SLB RADIUS framed-IP sticky database, configure an **idle** command with the **radius framed-ip** keywords specified. • (Optional) To enable IOS SLB to create the IOS SLB RADIUS framed-IP sticky database and direct RADIUS requests and non-RADIUS flows from a subscriber to the same service gateway, specify the **sticky**command with the **radius framed-ip**keywords. If you configure the **sticky radius framed-ip**command, you must also configure the **virtual** command with the **service radius**keywords specified.
Step 3	Configure a virtual server. (continued)	• (Optional--for CDMA2000 networks only) To enable IOS SLB to create the IOS SLB RADIUS calling-station-ID sticky database and direct RADIUS requests from a subscriber to the same service gateway based on the calling station ID, specify the **sticky**command with the **radius calling-station-id**keywords.

	Command or Action	Purpose
		To enable IOS SLB to create the IOS SLB RADIUS username sticky database and direct RADIUS requests from a subscriber to the same service gateway based on the username, specify the **sticky**command with the **radius username**keywords. If you configure the **sticky radius calling-station-id**command or the **sticky radius username**command, you must also configure the **virtual** command with the **service radius**keywords specified, and you must configure the **sticky radius framed-ip**command. You cannot configure both the **sticky radius calling-station-id** command and the **sticky radius username** command on the same virtual server.
Step 4	Enable IOS SLB to inspect packets for RADIUS framed-IP sticky routing.	(Optional) See "How to Enable IOS SLB to Inspect Packets for RADIUS Framed-IP Sticky Routing".
Step 5	Configure RADIUS load balancing maps.	(Optional) See "How to Configure RADIUS Load Balancing Maps".
Step 6	Increase the number of available MLS entries.	(Optional
Step 7	Configure a probe.	See "How to Configure a Probe". To verify the health of the server, configure a ping probe.

Firewall Configuration for the Exchange Director

Perform this task to configure firewall load balancing for the Exchange Director.

This section lists the tasks used to configure firewalls for the Exchange Director. Detailed configuration information is contained in the referenced sections of this or other documents. Required and optional tasks are indicated.

- How to Configure a Firewall Farm, page 45
- How to Verify a Firewall Farm, page 49
- How to Verify Firewall Connectivity, page 50
- How to Configure a Probe, page 51
- How to Configure a Wildcard Search, page 52
- How to Configure Protocol-Level Purging of MLS entries, page 52
- How to Configure Connection Purge Request Behavior, page 52
- How to Configure Sticky Connection Purge Request Behavior, page 52

How to Configure a Firewall Farm

Perform the following required task to configure a firewall farm.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb firewallfarm** *firewall-farm*
4. **real** *ip-address*
5. **probe** *probe*
6. **weight** *setting*
7. **inservice**
8. **exit**
9. **access** [**source** *source-ip netmask*] [**destination** *destination-ip netmask*]| **inbound** *inbound-interface* | **outbound** *outbound-interface*]
10. **predictor hash address** [**port**]
11. **purge connection**
12. **purge sticky**
13. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [[*encrypt*] *secret-string* [*timeout*]]]
14. **protocol tcp**
15. **delay** *duration*
16. **idle** *duration*
17. **maxconns** *maximum-number*
18. **sticky** *seconds* [**netmask** *netmask*] [**source**| **destination**]
19. **exit**
20. **protocol datagram**
21. **idle** *duration*
22. **maxconns** *maximum-number*
23. **sticky** *seconds* [**netmask** *netmask*] [**source**| **destination**]
24. **exit**
25. **inservice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb firewallfarm** *firewall-farm*	Adds a firewall farm definition to the IOS SLB configuration and enters firewall farm configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# ip slb firewallfarm FIRE1`	
Step 4	**real** *ip-address* **Example:** `Router(config-slb-fw)# real 10.1.1.1`	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.
Step 5	**probe** *probe* **Example:** `Router(config-slb-fw-real)# probe FireProbe`	Associates a probe with the firewall.
Step 6	**weight** *setting* **Example:** `Router(config-slb-fw-real)# weight 16`	(Optional) Specifies the firewall's workload capacity relative to other firewalls in the firewall farm.
Step 7	**inservice** **Example:** `Router(config-slb-fw-real)# inservice`	Enables the firewall for use by the firewall farm and by IOS SLB.
Step 8	**exit** **Example:** `Router(config-slb-fw-real)# exit`	Exits real server configuration mode.
Step 9	**access** [**source** *source-ip netmask*] [**destination** *destination-ip netmask*]| **inbound** *inbound-interface* | **outbound** *outbound-interface*] **Example:** `Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0`	(Optional) Routes specific flows to a firewall farm.
Step 10	**predictor hash address** [**port**] **Example:** `Router(config-slb-fw)# predictor hash address`	(Optional) Specifies whether the source and destination TCP or User Datagram Protocol (UDP) port numbers, in addition to the source and destination IP addresses, are to be used when selecting a firewall.
Step 11	**purge connection**	(Optional) Enables IOS SLB firewall load balancing to send purge requests for connections.

	Command or Action	Purpose
	Example: `Router(config-slb-fw)# purge connection`	
Step 12	**purge sticky** **Example:** `Router(config-slb-fw)# purge sticky`	(Optional) Enables IOS SLB firewall load balancing to send purge requests when the sticky idle timer expires.
Step 13	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [[*encrypt*] *secret-string* [*timeout*]]] **Example:** `Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231`	(Optional) Configures a stateful backup of IOS SLB firewall load balancing decision tables to a backup switch.
Step 14	**protocol tcp** **Example:** `Router(config-slb-fw)# protocol tcp`	(Optional) Enters firewall farm TCP protocol configuration mode.
Step 15	**delay** *duration* **Example:** `Router(config-slb-fw-tcp)# delay 30`	(Optional) For firewall farm TCP protocol configuration mode, specifies the time IOS SLB firewall load balancing maintains TCP connection context after a connection has ended.
Step 16	**idle** *duration* **Example:** `Router(config-slb-fw-tcp)# idle 120`	(Optional) For firewall farm TCP protocol configuration mode, specifies the minimum time IOS SLB firewall load balancing maintains connection context in the absence of packet activity.
Step 17	**maxconns** *maximum-number* **Example:** `Router(config-slb-fw-tcp)# maxconns 1000`	(Optional) For firewall farm TCP protocol configuration mode, specifies the maximum number of active TCP connections allowed on the firewall farm at one time.
Step 18	**sticky** *seconds* [**netmask** *netmask*] [**source**| **destination**] **Example:** `Router(config-slb-fw-tcp)# sticky 60`	(Optional) For firewall farm TCP protocol configuration mode, specifies that connections from the same IP address use the same firewall if either of the following conditions is met: • As long as any connection between the same pair of IP addresses exists (source and destination sticky). • For a period, defined by *duration* , after the last connection is destroyed.
Step 19	**exit**	Exits firewall farm TCP protocol configuration mode.

	Command or Action	Purpose
	Example: `Router(config-slb-fw-tcp)# exit`	
Step 20	**protocol datagram** **Example:** `Router(config-slb-fw)# protocol datagram`	(Optional) Enters firewall farm datagram protocol configuration mode.
Step 21	**idle** *duration* **Example:** `Router(config-slb-fw-udp)# idle 120`	(Optional) For firewall farm datagram protocol configuration mode, specifies the minimum time IOS SLB firewall load balancing maintains connection context in the absence of packet activity.
Step 22	**maxconns** *maximum-number* **Example:** `Router(config-slb-fw-udp)# maxconns 1000`	(Optional) For firewall farm datagram protocol configuration mode, specifies the maximum number of active datagram connections allowed on the firewall farm at one time.
Step 23	**sticky** *seconds* [**netmask** *netmask*] [**source**| **destination**] **Example:** `Router(config-slb-fw-udp)# sticky 60`	(Optional) For firewall farm datagram protocol configuration mode, specifies that connections from the same IP address use the same firewall if either of the following conditions is met: • As long as any connection between the same pair of IP addresses exists (source and destination sticky). • For a period, defined by *duration* , after the last connection is destroyed.
Step 24	**exit** **Example:** `Router(config-slb-fw-udp)# exit`	Exits firewall farm datagram protocol configuration mode.
Step 25	**inservice** **Example:** `Router(config-slb-fw)# inservice`	Enables the firewall farm for use by IOS SLB.

How to Verify a Firewall Farm

Perform the following optional task to verify a firewall farm.

SUMMARY STEPS

1. The following **show ip slb reals** command displays the status of firewall farm FIRE1, the associated real servers, and their status:
2. The following **show ip slb firewallfarm**command displays the configuration and status of firewall farm FIRE1:

DETAILED STEPS

Step 1 The following **show ip slb reals** command displays the status of firewall farm FIRE1, the associated real servers, and their status:

Example:

```
Router# show ip slb real
real                farm name        weight   state          conns
-------------------------------------------------------------------
10.1.1.2            FIRE1            8        OPERATIONAL    0
10.1.2.2            FIRE1            8        OPERATIONAL    0
```

Step 2 The following **show ip slb firewallfarm**command displays the configuration and status of firewall farm FIRE1:

Example:

```
Router# show ip slb firewallfarm
firewall farm    hash        state         reals
-----------------------------------------------
FIRE1            IPADDR      INSERVICE     2
```

How to Verify Firewall Connectivity

Perform the following optional task to verify firewall connectivity.

To verify that IOS SLB firewall load balancing is configured and operating correctly, perform the following steps:

SUMMARY STEPS

1. Ping the external real servers (the ones outside the firewall) from the IOS SLB firewall load-balancing device.
2. Ping the internal real servers (the ones inside the firewall) from the clients.
3. Use the **show ip slb stats** command to display information about the IOS SLB firewall load-balancing network status:
4. Use the **show ip slb real detail**command to display detailed information about the IOS SLB firewall load-balancing real server status:
5. Use the **show ip slb conns**command to display information about active IOS SLB firewall load-balancing connections:

DETAILED STEPS

Step 1 Ping the external real servers (the ones outside the firewall) from the IOS SLB firewall load-balancing device.

Step 2 Ping the internal real servers (the ones inside the firewall) from the clients.

Step 3 Use the **show ip slb stats** command to display information about the IOS SLB firewall load-balancing network status:

Example:

```
Router# show ip slb stats
```

```
 Pkts via normal switching:  0
 Pkts via special switching: 0
 Pkts dropped:               0
 Connections Created:        1911871
 Connections Established:    1967754
 Connections Destroyed:      1313251
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         59752
 Connection Flowcache Purges:1776582
 Failed Connection Allocs:   17945
 Failed Real Assignments:    0
```

- Normal switching exists when IOS SLB packets are managed on normal IOS switching paths (CEF, fast switching, and process level switching).
- Special switching exists when IOS SLB packets are managed on hardware-assisted switching paths.

Step 4 Use the **show ip slb real detail**command to display detailed information about the IOS SLB firewall load-balancing real server status:

Example:

```
Router# show ip slb reals detail
172.16.88.5, SF1, state = OPERATIONAL, type = server
  ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

Step 5 Use the **show ip slb conns**command to display information about active IOS SLB firewall load-balancing connections:

Example:

```
Router# show ip slb conns
vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
```

For additional commands used to verify IOS SLB networks and connections, see "How to Monitor and Maintain the Cisco IOS SLB Feature".

How to Configure a Probe

Perform the following required task to configure a probe.

The Exchange Director uses probes to detect and recover from failures. You must configure a probe on each real server in the firewall farm.

- We recommend ping probes for each real server in a firewall farm. For more details, see "How to Configure a Ping Probe".
- If a firewall does not allow ping probes to be forwarded, use HTTP probes instead. For more details, see "How to Configure an HTTP Probe".

- You can configure more than one probe, in any combination of supported types (DNS, HTTP, TCP, or ping), for each firewall in a firewall farm.

How to Configure a Wildcard Search

How to Configure Protocol-Level Purging of MLS entries

To disable purge throttling on TCP and UDP flow packets, use the **no** form of this command.

How to Configure Connection Purge Request Behavior

To completely stop the sending of purge requests, use the **no** form of this command.

How to Configure Sticky Connection Purge Request Behavior

To completely stop the sending of purge requests for sticky connections, use the **no** form of this command.

VPN Server Load Balancing Configuration Task List

SUMMARY STEPS

1. Configure a server farm and a real server.
2. Configure a virtual server.
3. Configure a probe.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for VPN server load balancing, specify the IP addresses of the real servers acting as VPN terminators using the **real** command.
Step 2	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the virtual server for VPN server load balancing of IPSec flows, keep the following considerations in mind: • Configure a UDP virtual server using the **virtual** command with the protocol set to **udp** and the port set to **isakmp**. The **isakmp** keyword enables the cryptographic key exchange to occur through IKE (port 500). • Configure an ESP virtual server using the **virtual** command with the protocol set to **esp**. • Specify a sticky connection from the UDP virtual server to the ESP virtual server, and vice versa, using the **sticky** command with a *duration* of at least 15 seconds. When you configure the virtual server for VPN server load balancing of Point-to-Point Tunneling Protocol (PPTP) flows, keep the following considerations in mind:

	Command or Action	Purpose
		• Configure a TCP virtual server, using the **virtual** command with the **tcp** keyword and port number **1723** specified. • Configure a GRE virtual server, using the **virtual** command with the **gre** keyword specified. • Specify a sticky connection from the TCP virtual server to the GRE virtual server, and vice versa, using the **sticky** command with a *duration* of at least 15 seconds.
Step 3	Configure a probe.	See "How to Configure a Probe". To verify the health of the server, configure a ping probe.

ASN Load Balancing Configuration Task List

Perform the following task to configure load balancing across a set of Access Service Network (ASN) gateways.

SUMMARY STEPS

1. Configure the base station.
2. Configure a probe.
3. Associate a server farm and a real server with the probe.
4. Associate a virtual server with the server farm.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure the base station.	To enable IOS SLB to manage requests from the Mobile Subscriber Station (MSS), configure the base station with the virtual IP address of the IOS SLB device.
Step 2	Configure a probe.	See "How to Configure a Probe". To verify the health of the server, configure a ping probe.
Step 3	Associate a server farm and a real server with the probe.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for ASN load balancing, keep the following considerations in mind: • Specify the IP addresses of the ASN gateways, using the **real** command. • (Optional) Enable IOS SLB to automatically remove objects associated with failed real servers from the ASN sticky database, using the **asn purge** option on the **real** command.
Step 4	Associate a virtual server with the server farm.	See "How to Configure a Virtual Server". When you configure the virtual server for ASN load balancing, keep the following considerations in mind: • Configure a virtual server, using the **virtual** command with the service set to **asn**. • Configure an idle connection timer for ASN load balancing, using the **idle** command with the **asn request** keywords specified. • (Optional) Enable IOS SLB to load-balance ASN sessions for a given MSID, using the **asn msid** option on the **sticky** command.

	Command or Action	Purpose
		• (Optional) Configure a timer for the ASN MSID sticky database, using the **idle** command with the **asn msid** keywords specified. • (Optional) Configure a Cisco BWG port, using the **gw port** command.

Home Agent Director Configuration Task List

Perform the following task to configure the Home Agent Director.

SUMMARY STEPS

1. Configure a server farm and a real server.
2. Configure a virtual server.
3. Configure the virtual IP address as a loopback on each of the home agents in the servers.
4. Configure DFP.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure a server farm and a real server.	See "How to Configure a Server Farm and a Real Server". When you configure the server farm and real server for the Home Agent Director, keep the following considerations in mind: • Accept the default setting (the weighted round robin algorithm) for the **predictor** command. • Specify the IP addresses of the real servers acting as home agents, using the **real** command.
Step 2	Configure a virtual server.	See "How to Configure a Virtual Server". When you configure the virtual server for the Home Agent Director using the **virtual** command, keep the following considerations in mind: • Specify the Home Agent Director's IP address as the virtual server. • Specify the **udp** keyword option. • Specify port number 434 if the home agents are in compliance with the IP Mobility Support, RFC 2002, or specify port number 0 or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports). • Specify the **service ipmobile**keyword option.
Step 3	Configure the virtual IP address as a loopback on each of the home agents in the servers.	(Required for dispatched mode) This step is required only if you are using dispatched mode. Refer to the "Configuring a Loopback Interface" section in the *Cisco IOS Interface Configuration Guide* , Release 12.2 for more information.
Step 4	Configure DFP.	(Optional) See "How to Configure DFP". When you configure DFP for the Home Agent Director, keep the following considerations in mind:

	Command or Action	Purpose
		• To control the maximum DFP weight sent by the home agent to IOS SLB, use the **ip mobile home-agent dfp-max-weight** command. • To set the source address and home agent address field in the Registration Reply (RRP) as the real home agent's address, use the **ip mobile home-agent dynamic-address**command. • To set the maximum number of bindings, use the **ip mobile home-agent max-binding** command. For information about these Mobile IP commands, refer to the *Cisco Mobile Wireless Home Agent Release 2.0* feature module.

How to Configure NAT

Perform the following task to configure the IOS SLB Network Address Translation (NAT) client address pool for client NAT.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb natpool pool** *start-ip end-ip* [**netmask** *netmask* | **prefix-length** *leading-1-bits*] [**entries** *init-address* [*max-address*]]
4. **nat** {**client** *pool* | **server**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb natpool pool** *start-ip end-ip* [**netmask** *netmask* | **prefix-length** *leading-1-bits*] [**entries** *init-address* [*max-address*]] **Example:** `Router(config)# ip slb natpool web-clients 10.1.10.1 10.1.10.5 netmask 255.255.0.0`	Configures the client address pool. GPRS load balancing does not support this command. You do not need to configure the client address pool for server NAT.

	Command or Action	Purpose
Step 4	**nat** {**client** *pool* | **server**} **Example:** `Router(config-slb-sfarm)# nat server`	Configures SLB NAT and specifies a NAT mode. All IPv4 or IPv6 server farms that are associated with the same virtual server must have the same NAT configuration.

You must also specify either NAT client translation mode or NAT server address translation mode on the server farm, using the **nat**command. See "How to Configure a Server Farm and a Real Server" for more details. When you configure the virtual server for NAT, remember that you cannot configure client NAT for an ESP or GRE virtual server.

How to Configure Static NAT

Perform the following task to configure static NAT.

Static NAT enables you to allow some users to use NAT and allow other users on the same Ethernet interface to continue with their own IP addresses. This option enables you to provide a default NAT behavior for real servers, differentiating between responses from a real server, and connection requests initiated by the real server.

Note To avoid unexpected results, make sure your static NAT configuration mirrors your virtual server configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb static** {**drop** | **nat** {**virtual** | *virtual-ip*[**per-packet** | **sticky**]}}
4. **real** *ip-address* [*port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip slb static** {**drop** | **nat** {**virtual** | *virtual-ip*[**per-packet** | **sticky**]}} **Example:** `Router(config)# ip slb static nat 10.1.10.1 per-packet`	Configures the real server's NAT behavior and enters static NAT configuration mode. **Note** If you specify the *virtual-ip* argument and you do not specify the **per-packet** option, IOS SLB uses server port translation to distinguish between connection requests initiated by different real servers.
Step 4	**real** *ip-address* [*port*] **Example:** `Router(config-slb-static)# real 10.1.1.3`	Configures one or more real servers to use static NAT.

Stateless Backup Configuration Task List

Perform the following task to configure stateless backup over VLANs between IOS SLB devices.

Note For active standby, in which multiple IOS SLB devices share a virtual IP address, you must use exclusive client ranges and you must use policy routing to forward flows to the correct IOS SLB device.

SUMMARY STEPS

1. Configure required and optional IOS SLB functions.
2. Configure firewall load balancing.
3. Configure the IP routing protocol.
4. Configure the VLAN between the IOS SLB devices.
5. Verify the stateless backup configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure required and optional IOS SLB functions.	(Required for server load balancing) See "How to Configure Required and Optional IOS SLB Functions".
Step 2	Configure firewall load balancing.	(Required for firewall load balancing) See "How to Configure Firewall Load Balancing".
Step 3	Configure the IP routing protocol.	Refer to the "IP Routing Protocols" chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2 for details.
Step 4	Configure the VLAN between the IOS SLB devices.	Refer to the "Virtual LANs" chapter of the *Cisco IOS Switching Services Configuration Guide*, Release 12.2 for details.
Step 5	Verify the stateless backup configuration.	(Optional) See "How to Verify the Stateless Backup Configuration".

- How to Verify the Stateless Backup Configuration, page 58

How to Verify the Stateless Backup Configuration

Perform the following task to verify the stateless backup configuration.

For server load balancing, to verify that stateless backup has been configured and is operating correctly, use the following **show ip slb vservers** commands to display information about the IOS SLB virtual server status:

```
Router# show ip slb vservers
slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
VS1              TCP   10.10.10.12:23        OPERATIONAL     2
VS2              TCP   10.10.10.18:23        OPERATIONAL     2
Router# show ip slb vservers detail
VS1, state = OPERATIONAL, v_index = 10
  virtual = 10.10.10.12:23, TCP, service = NONE, advertise = TRUE
  server farm = SERVERGROUP1, delay = 10, idle = 3600
  sticky timer = 0, sticky subnet = 255.255.255.255
  sticky group id = 0
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 0, syns = 0, syn drops = 0
  standby group = None
VS2, state = INSERVICE, v_index = 11
  virtual = 10.10.10.18:23, TCP, service = NONE, advertise = TRUE
  server farm = SERVERGROUP2, delay = 10, idle = 3600
  sticky timer = 0, sticky subnet = 255.255.255.255
  sticky group id = 0
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 0, syns = 0, syn drops = 0
  standby group = None
```

For firewall load balancing, to verify that stateless backup has been configured and is operating correctly, use the following **show ip slb firewallfarm**commands to display information about the IOS SLB firewall farm status:

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-----------------------------------------------
FIRE1            IPADDR      INSERVICE     2
Router# show ip slb firewallfarm details
FIRE1, hash = IPADDRPORT, state = INSERVICE, reals = 2
  FirewallTCP:
   sticky timer = 0, sticky subnet = 255.255.255.255
   idle = 3600, delay = 10, syns = 1965732, syn drop = 0
   maxconns = 4294967295, conns = 597445, total conns = 1909512
  FirewallUDP:
   sticky timer = 0, sticky subnet = 255.255.255.255
   idle = 3600
   maxconns = 1, conns = 0, total conns = 1
  Real firewalls:
    10.1.1.3, weight = 10, OPERATIONAL, conns = 298823
    10.1.1.4, weight = 10, OPERATIONAL, conns = 298622
  Total connections = 597445
```

Stateful Backup of Redundant Route Processors Configuration Task List

SUMMARY STEPS

1. Configure the replication message rate for slave replication.
2. Configure required and optional IOS SLB functions.
3. Configure firewall load balancing.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Configure the replication message rate for slave replication.	Specify the **ip slb replicate slave rate**command in global configuration mode.
Step 2	Configure required and optional IOS SLB functions.	(Required for server load balancing) See "How to Configure Required and Optional IOS SLB Functions". When you configure the virtual server for stateful backup of redundant route processors, keep the following considerations in mind: • Specify the **replicate slave**command. • (Optional) To set the replication delivery interval for the virtual server, configure a **replicate interval**command.
Step 3	Configure firewall load balancing.	(Required for firewall load balancing) See "How to Configure Firewall Load Balancing". When you configure the firewall farm for stateful backup of redundant route processors, keep the following considerations in mind: • Specify the **replicate slave**command. • (Optional) To set the replication delivery interval for the firewall farm, configure a **replicate interval**command.

How to Configure Database Entries

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb entries** [**conn** [*init-conn* [*max-conn*]] | **frag** [*init-frag* [*max-frag*] | **lifetime** *timeout*] | **gtp** {**gsn** [*init-gsn*[*max-gsn*] | **nsapi** [*init-nsapi* [*max-nsapi*]} | **sticky** [*init-sticky* [*max-sticky*]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb entries** [**conn** [*init-conn* [*max-conn*]] | **frag** [*init-frag* [*max-frag*] | **lifetime** *timeout*] | **gtp** {**gsn** [*init-gsn*[*max-gsn*] | **nsapi** [*init-nsapi* [*max-nsapi*]} | **sticky** [*init-sticky* [*max-sticky*]]] **Example:** `Router(config)# ip slb entries conn 128000 512000`	Specifies an initial allocation and a maximum value for IOS SLB database entries. **Note** Enter this command *before* entering the rest of your IOS SLB configuration. If your IOS SLB configuration already exists, you must reload ISO SLB after entering this command.

How to Configure Buffers for the Fragment Database

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb maxbuffers frag** *buffers*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb maxbuffers frag** *buffers* **Example:** `Router(config)# ip slb maxbuffers frag 300`	Configures the maximum number of buffers for the IOS SLB fragment database.

How to Clear Databases and Counters

SUMMARY STEPS

1. **clear ip slb connections** [**firewallfarm** *firewall-farm*| **serverfarm** *server-farm*| **vserver** *virtual-server*]
2. **clear ip slb counters** [**kal-ap**]
3. **clear ip slb sessions** [**firewallfarm** *firewall-farm*| **serverfarm** *server-farm* | **vserver** *virtual-server*]
4. **clear ip slb sticky asn msid** *msid*
5. **clear ip slb sticky gtp imsi** [**id** *imsi*]
6. **clear ip slb sticky radius** {**calling-station-id** [**id** *string*] | framed-ip [*framed-ip* [*netmask*]]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear ip slb connections** [**firewallfarm** *firewall-farm*| **serverfarm** *server-farm*| **vserver** *virtual-server*] **Example:** `Router# clear ip slb connections vserver VSERVER1`	Clears the IOS SLB connection database for one or more firewall farms, server farms, or virtual servers.
Step 2	**clear ip slb counters** [**kal-ap**] **Example:** `Router# clear ip slb counters`	Clears the IOS SLB counters. Use the **kal-ap** keyword to clear only IP IOS SLB KeepAlive Application Protocol (KAL-AP) counters.
Step 3	**clear ip slb sessions** [**firewallfarm** *firewall-farm*| **serverfarm** *server-farm*	**vserver** *virtual-server*] **Example:** `Router# clear ip slb sessions serverfarm FARM1`	Clears the IOS SLB RADIUS session database for one or more firewall farms, server farms, or virtual servers.
Step 4	**clear ip slb sticky asn msid** *msid* **Example:** `Router# clear ip slb sticky asn msid 001646013fc0`	Clears entries from an IOS SLB Access Service Network (ASN) Mobile Station ID (MSID) sticky database.
Step 5	**clear ip slb sticky gtp imsi** [**id** *imsi*] **Example:** `Router# clear ip slb sticky gtp imsi`	Clears entries from an IOS SLB general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database.
Step 6	**clear ip slb sticky radius** {**calling-station-id** [**id** *string*]	framed-ip [*framed-ip* [*netmask*]]} **Example:** `Router# clear ip slb sticky radius framed-ip`	Clears entries from an IOS SLB RADIUS sticky database.

How to Configure a Wildcard Search

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **mls ip slb search**{**wildcard** [**pfc** | **rp**] | **icmp**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router(config)# **mls ip slb search**{**wildcard** [**pfc**	**rp**]	**icmp**} **Example:** `Router(config)# mls ip slb search wildcard rp`	Specifies the behavior of IOS SLB wildcard searches. This command is supported for Cisco Catalyst 6500 series switch only.

How to Configure Protocol-Level Purging of MLS Entries

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **mls ip slb purge global**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Router# configure terminal`	
Step 3	Router(config)# **mls ip slb purge global** **Example:** `Router(config)# mls ip slb purge global`	Specifies protocol-level purging of MLS entries from active TCP and UDP flow packets. This command is supported for Cisco Catalyst 6500 series switches only.

How to Purge and Reassign Connections

You can enable IOS SLB to automatically remove connections to failed real servers and firewalls from the connection database even if the idle timers have not expired. This function is useful for applications that do not rotate the source port (such as IKE), and for protocols that do not have ports to differentiate flows (such as ESP).

You can also enable IOS SLB to automatically reassign to a new real server or firewall RADIUS sticky objects that are destined for a failed real server or firewall.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **failaction** [**purge** | **asn purge**| **gtp purge**| **radius reassign**]
5. **exit**
6. **ip slb firewallfarm** *firewall-farm*
7. **failaction purge**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb serverfarm** *server-farm*	Enters server farm configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# ip slb serverfarm PUBLIC`	
Step 4	**failaction** [**purge** | **asn purge**| **gtp purge**| **radius reassign**] **Example:** `Router(config-slb-sfarm)# failaction purge`	Configures IOS SLB behavior in the event that a real server fails.
Step 5	**exit** **Example:** `Router(config-slb-sfarm)# exit`	Exits server farm configuration mode.
Step 6	**ip slb firewallfarm** *firewall-farm* **Example:** `Router(config)# ip slb firewallfarm fire1`	Enters firewall farm configuration mode.
Step 7	**failaction purge** **Example:** `Router(config-slb-fw)# failaction purge`	Configures IOS SLB behavior in the event that a firewall fails.

How to Disable Automatic Server Failure Detection

If you have configured all-port virtual servers (that is, virtual servers that accept flows destined for all ports except GTP ports), flows can be passed to servers for which no application port exists. When the servers reject these flows, IOS SLB might fail the servers and remove them from load balancing. This situation can also occur in slow-to-respond AAA servers in RADIUS load-balancing environments. To prevent this situation, you can disable automatic server failure detection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*]
5. **no faildetect inband**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip slb serverfarm** *server-farm* **Example:** `Router(config)# ip slb serverfarm PUBLIC`	Enters server farm configuration mode.
Step 4	**real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*] **Example:** `Router(config-slb-sfarm)# real 10.1.1.1`	Identifies a real server as a member of a server farm and enters real server configuration mode. **Note** For dual-stack support for GTP load balancing, specify the real server's IPv4 and IPv6 address.
Step 5	**no faildetect inband** **Example:** `Router(config-slb-real)# no faildetect inband`	Disables automatic server failure detection. **Note** If you disable automatic server failure detection using the **no faildetect inband** command, We recommend that you configure one or more probes. If you specify the **no faildetect inband** command, the **faildetect numconns** command is ignored, if specified.

How to Monitor and Maintain the Cisco IOS SLB Feature

Perform the following task to obtain and display runtime information about IOS SLB.

SUMMARY STEPS

1. **show ip slb conns** [**vserver** *virtual-server* | **client** *ip-address* | **firewall** *firewall-farm*] [**detail**]
2. **show ip slb dfp** [**agent** *agent-ip port* | **manager** *manager-ip* | **detail** | **weights**]
3. **show ip slb firewallfarm** [**detail**]
4. **show ip slb fragments**
5. **show ip slb gtp** {**gsn** [*gsn-ip-address*] | **nsapi** [*nsapi-key*] [**detail**]
6. **show ip slb map** [*map-id*]
7. **show ip slb natpool** [**name** *pool*] [**detail**]
8. **show ip slb probe** [**name** *probe*] [**detail**]
9. **show ip slb reals** [**sfarm** *server-farm*] [**detail**]
10. **show ip slb replicate**
11. **show ip slb serverfarms** [**name** *server-farm*] [**detail**]
12. **show ip slb sessions** [**asn**| **gtp**[**ipv6**] | **gtp-inspect**| **ipmobile**| **radius**] [**vserver** *virtual-server*] [**client** *ipv4-address netmask*] [**detail**]
13. **show ip slb static**
14. **show ip slb stats**
15. **show ip slb sticky** [**client** *ip-address netmask*| **radius calling-station-id**[**id** *string*] | **radius framed-ip**[**client** *ip-address netmask*] | **radius username**[**name** *string*]]
16. **show ip slb vservers** [**name** *virtual-server*] [**redirect**] [**detail**]
17. **show ip slb wildcard**

DETAILED STEPS

Step 1 **show ip slb conns** [**vserver** *virtual-server* | **client** *ip-address* | **firewall** *firewall-farm*] [**detail**]

Displays all connections managed by IOS SLB, or, optionally, only those connections associated with a particular virtual server or client. The following is sample output from this command:

Example:

```
Router# show ip slb conns
vserver          prot   client               real                 state
---------------------------------------------------------------------------
TEST             TCP    10.150.72.183:328    10.80.90.25:80       INIT
TEST             TCP    10.250.167.226:423   10.80.90.26:80       INIT
TEST             TCP    10.234.60.239:317    10.80.90.26:80       ESTAB
TEST             TCP    10.110.233.96:747     10.80.90.26:80       ESTAB
TEST             TCP    10.162.0.201:770      10.80.90.30:80       CLOSING
TEST             TCP    10.22.225.219:995     10.80.90.26:80       CLOSING
TEST             TCP    10.2.170.148:169      10.80.90.30:80
```

Step 2 **show ip slb dfp** [**agent** *agent-ip port* | **manager** *manager-ip* | **detail** | **weights**]

Displays information about Dynamic Feedback Protocol (DFP) and DFP agents, and about the weights assigned to real servers. The following is sample output from this command:

Example:

```
Router# show ip slb dfp
DFP Manager:
Current passwd:NONE Pending passwd:NONE
Passwd timeout:0 sec
```

```
Agent IP          Port    Timeout   Retry Count   Interval
-------------------------------------------------------------
172.16.2.34       61936   0         0             180 (Default)
```

Step 3 **show ip slb firewallfarm** [**detail**]
Displays information about firewall farms. The following is sample output from this command:

Example:

```
Router# show ip slb firewallfarm
firewall farm    hash        state         reals
-----------------------------------------------
FIRE1            IPADDR      OPERATIONAL     2
```

Step 4 **show ip slb fragments**
Displays information from the IOS SLB fragment database. The following is sample output from this command:

Example:

```
Router# show ip slb fragments
ip src          id    forward         src nat         dst nat
-------------------------------------------------------------------------
10.11.2.128     12    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     13    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     14    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     15    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     16    10.11.2.128     10.11.11.11     10.11.2.128
```

Step 5 **show ip slb gtp** {**gsn** [*gsn-ip-address*] | **nsapi** [*nsapi-key*] [**detail**]
Displays IOS SLB GPRS Tunneling Protocol (GTP) information. The following is sample output from this command:

Example:

```
Router# show ip slb gtp gsn 10.0.0.0
type ip              recovery-ie  purging
-----------------------------------------
SGSN 10.0.0.0 UNKNOWN      N
```

Step 6 **show ip slb map** [*map-id*]
Displays information about IOS SLB protocol maps. The following is sample output from this command:

Example:

```
Router# show ip slb map
ID: 1, Service: GTP
 APN: Cisco.com, yahoo.com
 PLMN ID(s): 11122, 444353
 SGSN access list: 100
ID: 2, Service: GTP
 PLMN ID(s): 67523, 345222
 PDP Type: IPv4, PPP
ID: 3, Service: GTP
 PDP Type: IPv6
ID: 4, Service: RADIUS
 Calling-station-id: “?919*”
ID: 5, Service: RADIUS
 Username: “. .778cisco.*”
```

Step 7 **show ip slb natpool** [**name** *pool*] [**detail**]
Displays information about the IOS SLB NAT configuration. The following is sample output from this command:

Example:

```
Router# show ip slb natpool
```

```
nat client B 209.165.200.225 1.1.1.6 1.1.1.8 Netmask 255.255.255.0
nat client A 10.1.1.1 1.1.1.5 Netmask 255.255.255.0
```

Step 8 **show ip slb probe** [**name** *probe*] [**detail**]

Displays information about probes defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb probe
Server:Port            State        Outages  Current  Cumulative
-----------------------------------------------------------------
10.10.4.1:0            OPERATIONAL        0  never    00:00:00
10.10.5.1:0            FAILED             1  00:00:06 00:00:06
```

Step 9 **show ip slb reals** [**sfarm** *server-farm*] [**detail**]

Displays information about the real servers defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb reals
real             farm name        weight   state           conns
-------------------------------------------------------------------------
10.80.2.112      FRAG             8        OUTOFSERVICE    0
10.80.5.232      FRAG             8        OPERATIONAL     0
10.80.15.124     FRAG             8        OUTOFSERVICE    0
10.254.2.2       FRAG             8        OUTOFSERVICE    0
10.80.15.124     LINUX            8        OPERATIONAL     0
10.80.15.125     LINUX            8        OPERATIONAL     0
10.80.15.126     LINUX            8        OPERATIONAL     0
10.80.90.25      SRE              8        OPERATIONAL     220
10.80.90.26      SRE              8        OPERATIONAL     216
10.80.90.27      SRE              8        OPERATIONAL     216
10.80.90.28      SRE              8        TESTING         1
10.80.90.29      SRE              8        OPERATIONAL     221
10.80.90.30      SRE              8        OPERATIONAL     224
10.80.30.3       TEST             100      READY_TO_TEST   0
10.80.30.4       TEST             100      READY_TO_TEST   0
10.80.30.5       TEST             100      READY_TO_TEST   0
10.80.30.6       TEST             100      READY_TO_TEST   0
```

Step 10 **show ip slb replicate**

Displays information about the IOS SLB replication configuration. The following is sample output from this command:

Example:

```
Router# show ip slb replicate

VS1, state = NORMAL, interval = 10
 Slave Replication: Enabled
 Slave Replication statistics:
  unsent conn updates:         0
  conn updates received:       0
  conn updates transmitted:    0
  update messages received:    0
  update messages transmitted: 0
 Casa Replication:
  local = 10.1.1.1 remote = 10.2.2.2 port = 1024
  current password = <none> pending password = <none>
  password timeout = 180 sec (Default)
 Casa Replication statistics:
  unsent conn updates:        0
  conn updates received:      0
  conn updates transmitted:   0
  update packets received:    0
  update packets transmitted: 0
  failovers:                  0
```

Step 11 **show ip slb serverfarms** [**name** *server-farm*] [**detail**]

Displays information about the server farms defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb serverfarms
server farm      predictor     reals   bind id
-----------------------------------------------
FRAG             ROUNDROBIN    4       0
LINUX            ROUNDROBIN    3       0
SRE              ROUNDROBIN    6       0
TEST             ROUNDROBIN    4       0
```

Step 12 **show ip slb sessions** [**asn**| **gtp**[**ipv6**] | **gtp-inspect**| **ipmobile**| **radius**] [**vserver** *virtual-server*] [**client** *ipv4-address netmask*] [**detail**]

Displays information about sessions managed by IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb sessions radius
Source              Dest                  Retry
Addr/Port           Addr/Port           Id Count  Real            Vserver
-------------------------------------------------------------------------------
10.10.11.1/1645     10.10.11.2/1812     15     1  10.10.10.1  RADIUS_ACCT
```

Step 13 **show ip slb static**

Displays information about the IOS SLB server Network Address Translation (NAT) configuration. The following is sample output from this command:

Example:

```
Router# show ip slb static
real                    action         address         counter
-----------------------------------------------------------------
10.11.3.4               drop           0.0.0.0         0
10.11.3.1               NAT            10.11.11.11     3
10.11.3.2               NAT sticky     10.11.11.12     0
10.11.3.3               NAT per-packet 10.11.11.13     0
```

Step 14 **show ip slb stats**

Displays IOS SLB statistics. The following is sample output from this command:

Example:

```
Router# show ip slb stats
Pkts via normal switching:     779
Pkts via special switching:    0
Pkts via slb routing:          0
Pkts Dropped:                  4
Connections Created:           4
Connections Established:       4
Connections Destroyed:         4
Connections Reassigned:        5
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS Framed-IP Sticky Count: 0
RADIUS username Sticky Count:           0
RADIUS calling-station-id Sticky Count:  0
GTP IMSI Sticky Count:         0
Failed Correlation Injects:    0
Pkt fragments drops in ssv:    0
ASN MSID sticky count:         1
```

Step 15 **show ip slb sticky** [**client** *ip-address netmask*| **radius calling-station-id**[**id** *string*] | **radius framed-ip**[**client** *ip-address netmask*] | **radius username**[**name** *string*]]

Displays information about the sticky connections defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb sticky
client           netmask          group  real                 conns
-------------------------------------------------------------------
10.10.2.12       255.255.0.0      4097   10.10.3.2             1
```

Step 16 **show ip slb vservers** [**name** *virtual-server*] [**redirect**] [**detail**]

Displays information about the virtual servers defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb vservers
slb vserver      prot   virtual              state          conns
-------------------------------------------------------------------
TEST             TCP     10.80.254.3:80        OPERATIONAL    1013
TEST21           TCP     10.80.254.3:21        OUTOFSERVICE   0
TEST23           TCP     10.80.254.3:23        OUTOFSERVICE   0
```

Step 17 **show ip slb wildcard**

Displays information about the wildcard representation for virtual servers defined to IOS SLB. The following is sample output from this command:

Example:

```
Router# show ip slb wildcard
Interface Source Address         Port  Destination Address    Port  Prot
ANY       0.0.0.0/0              0     3.3.3.3/32             2123  UDP
ANY       0.0.0.0/0              0     3.3.3.3/32             0     UDP
ANY       0.0.0.0/0              0     0.0.0.0/0              0     ICMP
Interface: ANY
Source Address [Port]: : :/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[0]
Protocol: ICMPV6
Interface: ANY
Source Address [Port]: : :/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[2123]
Protocol: UDP
```