default (tracking)

To set the default values for a tracked list, use the **default** command in tracking configuration mode. To disable the defaults, use the **no** form of this command.

default {**delay** | **object** *object-number* | **threshold percentage**}

no default {**delay** | **object** *object-number* | **threshold percentage**}

Syntax Description

delay	Default delay value.
object *object-number*	Default object for the list. The *object-number* argument has a valid range of 1 to 1000.
threshold percentage	Default threshold percentage.

Command Default

No default values for a track list are set.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows how to configure a default threshold percentage:

```
Router(config)# track 3 list
Router(config-track)# default threshold percentage
```

Related Commands

Command	Description
show track	Displays tracking information.
threshold weight	Specifies a threshold weight for a tracked list.

Command	Description
track list threshold percentage	Tracks a list of objects as to the up and down object states using a threshold percentage.
track list threshold weight	Tracks a list of objects as to the up and down object states using a threshold weight.

default-state

To set the default state for a stub object, use the **default-state** command in tracking configuration mode. To reset the default state to its internal default state, use the **no** form of this command.

default-state {**up** | **down**}

no default-state {**up** | **down**}

Syntax Description

up	Sets the current default state of a stub object to up.
down	Sets the current default state of a stub object to down.

Command Default

Internal default state is the default.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **default-state** command to set the default state of a stub object that has been created by the **track stub** command. The stub object can be tracked and manipulated by an external process, Embedded Event Manager (EEM).

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

Examples

The following example shows how to create a stub object and configure a default state for the stub object:

```
track 2 stub
 default-state up
```

Related Commands

Command	Description
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

delay (firewall farm TCP protocol)

To change the amount of time the IOS Server Load Balancing (IOS SLB) maintains TCP connection context after a connection has terminated, use the **delay** command in firewall farm TCP protocol configuration mode. To restore the default delay timer, use the **no** form of this command.

delay *duration*

no delay

Syntax Description

duration	Delay timer duration in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.

Defaults

The default duration is 10 seconds.

Command Modes

Firewall farm TCP protocol configuration (config-slb-fw-tcp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The delay timer allows out-of-sequence packets and final acknowledgments (ACKs) to be delivered after a TCP connection ends. Do not set this value to zero (0).

If you are configuring a delay timer for HTTP flows, choose a low number such as 5 seconds as a starting point.

Examples

The following example specifies that IOS SLB maintains TCP connection context for 30 seconds after a connection has terminated:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# delay 30
```

Related Commands

Command	Description
protocol tcp	Enters firewall farm TCP protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

delay (tracking)

To specify a period of time to delay communicating state changes of a tracked object, use the **delay** command in tracking configuration mode. To disable the delay period, use the **no** form of this command.

delay {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}

no delay {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}

Syntax Description

up	Time to delay the notification of an up event.
down	Time to delay the notification of a down event.
seconds	Delay value, in seconds. The range is from 0 to 180. The default is 0.

Defaults

No delay time is configured for tracking.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)B.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command is available to all tracked objects.

If you specify, for example, **delay up 10 down 30**, then if the object state changes from down to up, clients tracking that object are notified after 10 seconds. If the object state changes from up to down, then clients tracking that object are notified after 30 seconds.

Examples

In the following example, the tracking process is tracking the IP-route threshold metric. The delay period to communicate the changes of a down event of the tracked object to the client process is set to 30 seconds.

```
track 1 ip route 10.22.0.0/16 metric threshold
 threshold metric up 16 down 20
 delay down 30
```

delay (virtual server)

To change the amount of time IOS Server Load Balancing (IOS SLB) maintains TCP connection context after a connection has terminated, use the **delay** command in SLB virtual server configuration mode. To restore the default delay timer, use the **no** form of this command.

delay {*duration* | **radius framed-ip** *duration*}

no delay {*duration* | **radius framed-ip** *duration*}

Syntax Description

duration	Delay timer duration for TCP connection context, in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.
radius framed-ip *duration*	Delay timer for RADIUS framed-ip sticky database, in seconds. The valid range is 1 to 43200 seconds. The default value is 10 seconds.

Defaults

The default duration for the TCP connection context is 10 seconds.
The default duration for the RADIUS framed-ip sticky database is 10 seconds.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(18)E	The **radius** and **framed-ip** keywords and the *duration* argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The TCP connection context delay timer allows out-of-sequence packets and final acknowledgments (ACKs) to be delivered after a TCP connection ends. Do not set this value to zero (0).

If you are configuring a TCP connection context delay timer for HTTP flows, choose a low number such as 5 seconds as a starting point.

For the Home Agent Director, the **delay** command has no meaning and is not supported.

Examples

The following example specifies that IOS SLB maintains TCP connection context for 30 seconds after a connection has terminated:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# delay 30
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.
virtual	Configures the virtual server attributes.

expect

To configure a status code or regular expression to expect information from the HTTP probe, use the **expect** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

expect [**status** *status-code*] [**regex** *expression*]

no expect [**status** *status-code*] [**regex** *expression*]

Syntax Description

status *status-code*	(Optional) Configures the expected HTTP status code. The valid range is 100 to 599. The default expected status code is 200.
regex *expression*	(Optional) Configures the regular expression expected in the HTTP response. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the "Understanding Regular Expressions" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

The default expected status code is 200.
There is no default expected regular expression.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(3a)E	The **regex** keyword and *expression* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **expect** command configures the expected status code or regular expression to be received from the servers. A real server is considered to have failed and is taken out of service if any of the following events occurs:

- A status number other than the expected one is received.
- The expected regular expression is not received in the first 2920 bytes of probe output. (IOS Server Load Balancing [IOS SLB] searches only the first 2920 bytes for the expected status code or regular expression.)
- The server fails to respond.

For IOS SLB firewall load balancing, configure the HTTP probe to expect status code 40l.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP configuration mode, and configures the HTTP probe to expect the status code 40l and the regular expression Copyright:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# expect status 401 regex Copyright
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

failaction (firewall farm)

To configure the IOS Server Load Balancing (IOS SLB) feature's behavior when a firewall fails, use the **failaction** command in firewall farm configuration mode.

failaction purge

Syntax Description

purge	Enables IOS SLB to automatically remove connections to failed firewalls from the connection database even if the idle timers have not expired.

Defaults

If you do not specify the **failaction** command, IOS SLB does not automatically remove connections to failed firewalls.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is useful for applications that do not rotate the source port (such as Internet Key Exchange [IKE]), and for protocols that do not have ports to differentiate flows (such as Encapsulation Security Payload [ESP]).

Examples

In the following example, IOS SLB removes all connections to failed firewalls in firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# failaction purge
```

failaction (server farm)

To configure IOS Server Load Balancing (IOS SLB) feature's behavior when a real server fails, use the **failaction** command in server farm configuration mode. To restore the default settings, use the **no** form of this command.

failaction {**purge** | **asn purge** | **gtp purge** | **radius reassign**}

no failaction {**purge** | **asn purge** | **gtp purge** | **radius reassign**}

Syntax Description

purge	Enables IOS SLB to automatically remove connections to failed real servers from the connection database even if the idle timers have not expired.
asn purge	Enables IOS SLB to automatically remove objects associated with failed real servers from the Access Service Network (ASN) sticky database, even if the idle timers have not expired.
gtp purge	Enables IOS SLB to automatically remove objects associated with failed real servers from the general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database, even if the idle timers have not expired.
radius reassign	Enables IOS SLB to automatically reassign to a new real server RADIUS sticky objects that are destined for a failed real server.

Defaults

If you do not specify the **failaction** command, IOS SLB does not perform the following actions:

- Remove connections to failed real servers
- Remove connections to objects associated with failed real servers
- Remove ASN or GPRS sticky objects (IOS SLB continues to assign new session requests to the failed real servers)
- Reassign RADIUS sticky objects

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.1(11b)E	The **radius reassign** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The **gtp purge** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	The **asn purge** keywords were added.

Usage Guidelines

This command is useful for applications that do not rotate the source port (such as Internet Key Exchange [IKE]), and for protocols that do not have ports to differentiate flows (such as Encapsulation Security Payload [ESP]).

You can specify **no failaction purge**, but it has no effect on the connection database.

If you specify **failaction radius reassign**, IOS SLB reassigns RADIUS sticky objects without seeing any new RADIUS messages. The assumption is that, in the event of a failure, the RADIUS proxy gateways can handle user flows without seeing the RADIUS messages. If the RADIUS proxy gateways cannot do so, do not specify the **failaction radius reassign** command.

Examples

In the following example, IOS SLB removes all connections to failed real servers in server farm PUBLIC:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# failaction purge
```

faildetect (custom UDP probe)

To specify the number of consecutive unacknowledged custom User Datagram Protocol (UDP) probes that constitute failure of the real server, use the **faildetect** command in custom UDP probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-probes*

no faildetect

Syntax Description

number-of-probes	Number of consecutive unacknowledged custom UDP probes allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default value is one (1) unacknowledged custom UDP probe.

Defaults

The default value is one (1) unacknowledged probe.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Examples

In the following example the unacknowledged custom UDP probe threshold is set to 16:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom User Datagram Protocol (UDP) probe name and enters custom UDP probe configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

faildetect (DNS probe)

To specify the conditions that indicate a server failure, use the **faildetect** command in DNS probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-probes*

no faildetect

Syntax Description

number-of-probes	Number of consecutive unacknowledged Domain Name System (DNS) probes allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default value is three (3) unacknowledged DNS probes.

Defaults

The default value is three (3) unacknowledged DNS probes.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example the unacknowledged DNS probe threshold is set to 16:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe dns	Configures a Domain Name System (DNS) probe name and enters DNS probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

faildetect (ping probe)

To specify the conditions that indicate a server failure, use the **faildetect** command in ping probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-pings*

no faildetect

Syntax Description

number-of-pings	Number of consecutive unacknowledged pings allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default is ten (10) unacknowledged pings.

Defaults

The default value is ten (10) unacknowledged pings.

Command Modes

Ping probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example the unacknowledged ping threshold is set to 16:

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe ping	Configures a ping probe name and enters ping probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

faildetect inband (real server)

To enable automatic server failure detection, use the **faildetect inband** command in real server configuration mode. To disable automatic server failure detection, use the **no** form of this command.

faildetect inband

no faildetect inband

Syntax Description

This command has no arguments or keywords.

Defaults

Automatic server failure detection is enabled.

Command Modes

Real server configuration (config-slb-real)

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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, Cisco 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 using the **no faildetect inband** command.

Note If you disable automatic server failure detection using the **no faildetect inband** command, Cisco strongly recommends that you configure one or more probes.

If you specify the **no faildetect inband** command, the **faildetect numconns** command is ignored, if specified.

Examples

In the following example, automatic server failure detection is disabled:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# no faildetect inband
```

Related Commands

Command	Description
faildetect numconns (real server)	Specifies the conditions that indicate a real server failure.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

faildetect numconns (real server)

To specify the conditions that indicate a real server failure, use the **faildetect numconns** command in SLB real server configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect numconns *number-of-conns* [**numclients** *number-of-clients*]

no faildetect numconns *number-of-conns* [**numclients** *number-of-clients*]

Syntax Description

number-of-conns	Number of consecutive connection failures allowed before IOS Server Load Balancing (IOS SLB) fails the real server. The valid range is 1 to 255. The default value is 8.
numclients *number-of-clients*	(Optional) Number of unique client IP addresses that can experience connection failures before IOS SLB fails the real server. The valid range is 1 to 8. The default value is 2. If there is only one client in your network (for example, one serving GPRS support node [SGSN] in a general packet radio service [GPRS] load-balancing environment), then you must specify **numclients 1**. In RADIUS load balancing, for automatic session-based failure detection, specify **numclients 1**.

Defaults

If you do not specify the **faildetect numconns** command, the default value of the connection failure threshold is 8.
If you specify the **faildetect numconns** command but do not specify the **numclients** keyword, the default value of the client connection failure threshold is 2.

Command Modes

SLB real server configuration (config-slb-real)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(9)E	This command was modified to support GPRS load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you specify the **no faildetect inband** command, the **faildetect numconns** command is ignored, if specified.

IOS SLB does not fail the real server until both of the following conditions are met:

- There have been *number-of-conns* consecutive connection failures.
- There have been *number-of-clients* unique client connection failures.

That is, there can be many consecutive connection failures, but until there have also been *number-of-clients* unique client connection failures, IOS SLB does not fail the real server.

Similarly, there can be many unique client connection failures, but until there have also been *number-of-conns* consecutive connection failures, IOS SLB does not fail the real server.

GPRS load balancing has the following features:

- The **numconns** keyword specifies the number of consecutive Create Packet Data Protocol (PDP) requests allowed before IOS SLB fails the gateway GPRS support node (GGSN).
- The **numclients** keyword specifies the number of unique client Create PDP request failures allowed before IOS SLB fails the GGSN.

Examples

In the following example, the **numconns** keyword is set to 10 and the **numclients** keyword is set to 3:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# faildetect numconns 10 numclients 3
```

With those settings, IOS SLB will not fail the real server until there have been ten (10) consecutive connection failures and there have been three (3) unique client connection failures.

Related Commands

Command	Description
faildetect inband (real server)	Enables automatic server failure detection.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

farm-weight

To specify a weight to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when calculating the load value for a server farm, use the **farm-weight** command in server farm configuration mode. To restore the default weight value, use the **no** form of this command.

farm-weight *setting*

no farm-weight

Syntax Description

setting	Weight setting to be used by the KAL-AP agent. Valid settings range from 1 to 4294967295.

Defaults

If you do not configure a KAL-AP farm weight, IOS SLB calculates a relative weight.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

Configuring a **farm-weight** enables KAL-AP to calculate loads more accurately when load balancing in a global server load balancing (GSLB) environment.

For best results, configure a **farm-weight** that is equal to the sum of the maximum DFP weights for the real servers in the server farm. (The maximum DFP weight for a real server is configured using the **gprs dfp max-weight** command in global configuration mode.) For example, if there are three real servers in a server farm, configured with maximum DFP weights of 100, 50, and 50, then configure a **farm-weight** of 200 (that is, 100 + 50 + 50). If a real server is added to or removed from the server farm, you must adjust the **farm-weight** accordingly.

Examples

The following example specifies that a weight of 16 is to be used by the KAL-AP agent when calculating the load value for a server farm:

```
Router(config-slb-sfarm)# farm-weight 16
```

Related Commands

Command	Description
gprs dfp max-weight	Specifies the maximum weight sent to a DFP manager by a Gateway GPRS Support Node (GGSN) acting as a DFP agent.
ip slb capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.
ip slb serverfarm	Identifies a server farm and enter SLB server farm configuration mode.

forwarding-agent

To specify the port on which the forwarding agent will listen for wildcard and fixed affinities, use the **forwarding-agent** command in CASA-port configuration mode. To disable listening on that port, use the **no** form of this command.

forwarding-agent *port-number* [*password* [*timeout*]]

no forwarding-agent

Syntax Description

port-number	Port numbers on which the forwarding agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
password	(Optional) Text password used for generating the MD5 digest.
timeout	(Optional) Duration (in seconds) during which the Forwarding Agent will accept the new and old password. Valid range is from 0 to 3600 seconds. The default is 180 seconds.

Defaults

The default password timeout is 180 seconds.

The default port for the services manager is 1637.

Command Modes

CASA-port configuration (config-casa)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that the forwarding agent will listen for wildcard and fixed affinities on port 1637:

```
forwarding-agent 1637
```

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

no glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

Syntax Description

group-number	GLBP group number in the range from 0 to 1023.
text *string*	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	The **md5** keyword and associated parameters were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The same authentication method must be configured on all the routers that are configured to be members of the same GLBP group, to ensure interoperation. A router will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

Examples

The following example configures stringxyz as the authentication string required to allow GLBP routers in group 10 to interoperate:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain "AuthenticateGLBP" to obtain the current live key and key ID for the specified key chain:

```
Router(config)# key chain AuthenticateGLBP
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
service password-encryption	Encrypts passwords.

glbp client-cache maximum

To enable the Gateway Load Balancing Protocol (GLBP) client cache, use the **glbp client-cache** command in interface configuration mode. To disable a GLBP client cache, use the **no** form of this command.

glbp *group* **client-cache maximum** *number* [**timeout** *minutes*]

no glbp *group-number* **client-cache maximum** *number* [**timeout** *minutes*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
number	Specifies the maximum number of clients the cache will hold for this GLBP group. The range is from 8 to 2000.
timeout *minutes*	(Optional) The maximum amount of time, in minutes, a client entry can stay in the GLBP client cache after the client information was last updated. The range is from 1 to 1440.

Command Default

The GLBP client cache is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command enables a GLBP client cache on a single group only. To enable the client cache on multiple GLBP groups, you must apply this command to each group for which a client cache is required.

You must specify a maximum number of clients that the client cache will hold for a GLBP group to limit the size of the cache. If a GLBP client cache already exists when this command is entered and there are already more clients in the cache than the required number, all of the existing cache entries are discarded.

If you enter the **no** form of this command when there are already client entries in the cache, all of the client entries are discarded before the GLBP client cache is disabled.

Note For IPv4 networks, Cisco recommends setting a GLBP client cache timeout value that is slightly longer than the maximum expected end-host Address Resolution Protocol (ARP) cache timeout value.

Examples

The following example shows how to enable a GLBP client cache with a maximum of 1200 clients:

```
Router(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp forwarder preempt

To configure a router to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]

no glbp *group* **forwarder preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the router preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
glbp 10 forwarder preempt delay minimum 60
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ip

To activate the Gateway Load Balancing Protocol (GLBP), use the **glbp ip** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

glbp *group* **ip** [*ip-address* [**secondary**]]

no glbp *group* **ip** [*ip-address* [**secondary**]]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
ip-address	(Optional) Virtual IP address for the GLBP group. The IP address must be in the same subnet as the interface IP address.
secondary	(Optional) Indicates that the IP address is a secondary GLBP virtual address.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **glbp ip** command activates GLBP on the configured interface. If an IP address is specified, that address is used as the designated virtual IP address for the GLBP group. If no IP address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IP address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ip** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example activates GLBP for group 10 on Fast Ethernet interface 0/0. The virtual IP address to be used by the GLBP group is set to 10.21.8.10.

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 ip 10.21.8.10
```

The following example activates GLBP for group 10 on Fast Ethernet interface 0/0. The virtual IP address used by the GLBP group will be learned from another router configured to be in the same GLBP group.

```
interface fastethernet 0/0
 glbp 10 ip
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

glbp *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]

no glbp *group* **load-balancing**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
host-dependent	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
round-robin	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default

The round-robin method is the default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T2	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.0(1)M1	This command was modified. When the **no** form of this command is configured, if the AVG does not have an Active Virtual Forwarder (AVF), it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.1(2)T	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.

Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same router. Use the weighted method of GLBP load balancing when you need unequal load balancing because routers in the GLBP group have different forwarding capacities.

Examples

The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip 10.21.8.10
Router(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

glbp *group-number* **name** *group-name*

no glbp *group-number* **name** *group-name*

Syntax Description

group-number	GLBP group number. Range is from 0 to 1023.
group-name	GLBP group name specified as a character string. Maximum number of characters is 255.

Defaults

IP redundancy for a group is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

Examples

The following example assigns the abccomp name to GLBP group 10:

```
glbp 10 name abccomp
```

Related Commands

Command	Description
glbp authentication	Configures an authentication string for the GLBP.
glbp forwarder preempt	Configures a router to take over as AVF for a GLBP group if it has higher priority than the current AVF.
glbp ip	Activates GLBP.
glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.

Command	Description
glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
glbp priority	Sets the priority level of the gateway within a GLBP group.
glbp timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **preempt** [**delay minimum** *seconds*]

no glbp *group* **preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

A GLBP router with a higher priority than the current AVG cannot assume the role of AVG. The default delay value is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
glbp 10 preempt delay minimum 60
glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the router within a GLBP group.

glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

glbp *group* **priority** *level*

no glbp *group* **priority** *level*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
level	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Command Default

The GLBP virtual gateway preemptive scheme is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

Examples

The following example shows a virtual gateway being configured with a priority of 254:

```
glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp preempt	Configures a router to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp sso

To enable Gateway Load Balancing Protocol (GLBP) support of Stateful Switchover (SSO) if it has been disabled, use the **glbp sso** command in global configuration mode. To disable GLBP support of SSO, use the **no** form of this command.

glbp sso

no glbp sso

Syntax Description

This command has no arguments or keywords.

Command Default

GLBP Support for SSO is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to enable GLBP support of SSO if it has been manually disabled by the **no glbp sso** command.

Examples

The following example show how to disable GLBP support of SSO:

```
Router(config)# no glbp sso
```

Related Commands

Command	Description
debug glbp events	Displays debugging messages about GLBP events.
show glbp	Displays GLBP information.

glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

glbp *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no glbp *group* **timers**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
msec	(Optional) Specifies that the following (*hellotime* or *holdtime)* argument value will be expressed in milliseconds rather than seconds.
hellotime	Hello interval. The default is 3 seconds (3000 milliseconds).
holdtime	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).

Defaults

hellotime: 3 seconds
holdtime: 10 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Routers on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All routers in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, (*holdtime* > 3 * *hellotime*). The range of values for holdtime force the holdtime to be greater than the hello time.

Examples

The following example shows the GLBP group 10 on Fast Ethernet interface 0/0 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip
Router(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp timers redirect

To configure the time during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF), use the **glbp timers redirect** command in interface configuration mode. To restore the redirect timers to their default values, use the **no** form of this command.

glbp *group* **timers redirect** *redirect timeout*

no glbp *group* **timers redirect** *redirect timeout*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
redirect	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). **Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.
timeout	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

redirect: 600 seconds (10 minutes)
timeout: 14,400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. If the virtual forwarder has learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.

The redirect timer sets the time delay between a forwarder failing on the network and the AVG assuming that the forwarder will not return. The virtual MAC address to which the forwarder was responsible for replying is still given out in Address Resolution Protocol (ARP) replies, but the forwarding task is handled by another router in the GLBP group.

Note The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.

The timeout interval is the time delay between a forwarder failing on the network and the MAC address for which the forwarder was responsible becoming inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. The timeout interval must be long enough to allow all hosts to refresh their ARP cache entry that contained the virtual MAC address.

Examples

The following example shows the commands used to configure GLBP group 1 on Fast Ethernet interface 0/0 with a redirect timer of 1800 seconds (30 minutes) and timeout interval of 28,800 seconds (8 hours):

```
Router# config terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# glbp 1 timers redirect 1800 28800
```

glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no** form of this command.

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]

no glbp *group* **weighting**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
maximum	Maximum weighting value in the range from 1 to 254. Default value is 100.
lower *lower*	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper *upper*	(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Command Default

The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the router fails, the weighting value of the router may fall from the maximum value to below the lower threshold, causing the router to give up its role as a virtual forwarder. When the weighting value of the router rises above the upper threshold, the router can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a router goes down, the weighting for the router can be reduced by a specified value.

Examples

The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 weighting 110 lower 95 upper 105
```

Related Commands

Command	Description
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	Configures an interface to be tracked.

glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

glbp *group* **weighting track** *object-number* [**decrement** *value*]

no glbp *group* **weighting track** *object-number* [**decrement** *value*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
object-number	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the **track** command to configure the tracked object.
decrement *value*	(Optional) Specifies an amount by which the GLBP weighting for the router is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

Command Default

Objects are not tracked for GLBP weighting changes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, Fast Ethernet interface 0/0 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting track 1
Router(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

gtp notification cac

To limit the number of times IOS SLB can reassign a session to a new real server for GGSN-IOS SLB messaging, use the **gtp notification cac** command in virtual server configuration mode. To restore the default limit, use the **no** form of this command.

gtp notification cac [*reassign-count*]

no gtp notification cac

Syntax Description

reassign-count	(Optional) Number of times IOS SLB can reassign a session to a new real server. That is, the number of times that IOS SLB can reassign a rejected Create PDP Context to a new real GGSN. The valid range is 1 to 20 reassignments. The default setting is 2 reassignments (that is, the initial real server assignment and 2 additional reassignments).

Defaults

The default is 2 reassignments (that is, the initial real server assignment and 2 additional reassignments).

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(17d)SXB1	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that IOS SLB can reassign a session up to 5 times:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# gtp notification cac 5
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

gtp session (virtual server)

To enable IOS SLB to create general packet radio service (GPRS) Tunneling Protocol (GTP) load-balancing sessions, use the **gtp session** command in SLB virtual server configuration mode. To disable the creation of GTP sessions by IOS SLB, (the sticky-only load-balancing solution), use the **no** form of this command.

gtp session

no gtp session

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB creates GTP load-balancing sessions.
Sticky-only load-balancing is disabled.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Sticky-only load balancing is supported for all versions of GTP.

If sticky-only load balancing (**no gtp session**) is enabled for GTP:

- IOS SLB load-balances GTP Packet Data Protocol (PDP) create requests based on the sticky objects in the GTP International Mobile Subscriber ID (IMSI) sticky database.
- Sticky connections must also be enabled for the virtual server, using the **sticky (virtual server)** command.
- Automatic server failure detection (the **faildetect inband** command) is not supported. Instead, use probes to detect real server failures.

Examples

The following example specifies that sticky-only load balancing is to be used for GTP:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no gtp session
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.
virtual	Configures the virtual server attributes.

gw port (virtual server)

To specify the port that the Cisco Broadband Wireless Gateway (BWG) is to use to communicate with IOS SLB, use the **gw port** command in SLB virtual server configuration mode. To restore the default settings, use the **no** form of this command.

gw port *port*

no gw port *port*

Syntax Description

port	Port number used by the Cisco BWG to communicate with IOS SLB. This port number must be unique across all virtual servers. Valid port numbers are 1 to 65535.

Defaults

No port number is defined.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The Cisco BWG uses this port when sending delete notifications and NAI update messages to IOS SLB.

If multiple communication ports are needed, the network administrator must identify multiple unique unused ports.

Examples

The following example specifies that the Cisco BWG is to use port 63082 to communicate with IOS SLB:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# gw port 63082
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.
virtual	Configures the virtual server attributes.

hand-off radius

To change the amount of time IOS Server Load Balancing (IOS SLB) waits for an ACCT-START message from a new Mobile IP foreign agent in the event of a foreign agent hand-off, use the **hand-off radius** command in virtual server configuration mode. To restore the default hand-off timer, use the **no** form of this command.

hand-off radius *duration*

no hand-off radius

Syntax Description

duration	Hand-off timer duration in seconds. The valid range is 1 to 43200 seconds.

Defaults

No default behavior or values

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The hand-off radius timer is valid only for RADIUS virtual servers that have the **service radius** keywords specified on the **virtual** command.

Examples

The following example specifies that IOS SLB waits for 30 seconds after a foreign agent hand-off:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# hand-off radius 30
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

header

To configure the basic authentication values for the HTTP probe, use the **header** command in HTTP probe configuration mode. To remove a header HTTP probe configuration, use the **no** form of this command.

header *field-name* [*field-value*]

no header *field-name* [*field-value*]

Syntax Description

field-name	Configures the name of the HTTP probe header. The character string is limited to 15 characters.
field-value	(Optional) Configures the value of the HTTP probe header.

Defaults

The following headers are inserted in the request by default:

Accept: */*
Connection: close
User-Agent: cisco-slb-probe/1.0
Host: *virtual IP address*

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **header** command in HTTP probe configuration mode configures the name and value parameters of the header.

Note The colon (:) separating the field name and field value is automatically inserted if not provided. Multiple headers with the same name are not supported.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP configuration mode, and configures the HTTP probe header name as HeaderName and value as HeaderValue:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# header HeaderName HeaderValue
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.