lookup

To configure an IP address of a real server that a Domain Name System (DNS) server should supply in response to a domain name resolve request, use the **lookup** command in DNS probe configuration mode. To remove an IP address from the expected list, use the **no** form of this command.

lookup *ip-address*

no lookup *ip-address*

Syntax Description

ip-address	IP address of a real server that a DNS server should supply in response to a domain name resolve request.

Defaults

No lookup IP address is configured.

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

The following example configures a DNS probe named PROBE4, enters DNS probe configuration mode, and specifies 10.1.10.1 as the IP address to resolve:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# lookup 10.1.10.1
```

Related Commands

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

manager (DFP agent)

This command has been removed. Its function is now performed by the **ip dfp agent** global configuration command, and by the following DFP agent configuration commands:

- **inservice (DFP agent)**
- **interval (DFP agent)**
- **password (DFP agent)**
- **port (DFP agent)**

See the description of these commands for more information.

maxclients

To specify the maximum number of IOS Server Load Balancing (IOS SLB) RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server, use the **maxclients** command in real server configuration mode. To remove the limit, use the **no** form of this command.

maxclients *maximum-number*

no maxclients

Syntax Description

maximum-number	Maximum number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server: • If the **radius calling-station-id** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS calling-station-ID sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS calling-station-ID sticky database. • If the **radius framed-ip** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS framed-IP sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS framed-IP sticky database. • If the **radius username** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS username sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS username sticky database. • If both the **radius framed-ip** and **radius calling-station-id** keywords are specified in the **sticky** command for the virtual server, a sticky subscriber is an entry in the IOS SLB RADIUS calling-station-ID sticky database. • If both the **radius framed-ip** and **radius username** keywords are specified in the **sticky** command for the virtual server, a sticky subscriber is an entry in the IOS SLB RADIUS username sticky database. By default, there is no limit on the number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server.

Defaults

There is no limit on the number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server.

Command Modes

Real server configuration (config-slb-real)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	This command was modified to support RADIUS load balancing for CDMA2000, a third-generation (3-G) version of Code Division Multiple Access (CDMA).
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

The following example specifies that up to 10 IOS SLB RADIUS sticky subscribers can be assigned to an individual real server:

```
Router(config-slb-real)# maxclients 10
```

Related Commands

Command	Description
ip slb route	Enables IOS SLB to inspect packets for RADIUS framed-IP sticky routing.
show ip slb sticky	Displays the IOS SLB sticky database.

maxconns (firewall farm datagram protocol)

To limit the number of active datagram connections to the firewall farm, use the **maxconns** command in firewall farm datagram protocol configuration mode. To restore the default of 4294967295, use the **no** form of this command.

maxconns *maximum-number*

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active datagram connections using the firewall farm. Valid values range from 1 to 4294967295. The default is 4294967295.

Defaults

The default maximum number of simultaneous active datagram connections using the firewall farm is 4294967295.

Command Modes

Firewall farm datagram protocol configuration (config-slb-fw-udp)

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

The following example limits the real server to a maximum of 1000 simultaneous active connections:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
Router(config-slb-fw-udp)# maxconns 1000
```

Related Commands

Command	Description
protocol datagram	Enters firewall farm datagram protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

maxconns (firewall farm TCP protocol)

To limit the number of active TCP connections to the firewall farm, use the **maxconns** command in firewall farm TCP protocol configuration mode. To restore the default of 4294967295, use the **no** form of this command.

maxconns *maximum-number*

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active TCP connections using the firewall farm. Valid values range from 1 to 4294967295. The default is 4294967295.

Defaults

The default maximum number of simultaneous active TCP connections using the firewall farm is 4294967295.

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.

Examples

The following example limits the real server to a maximum of 1000 simultaneous active connections:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# maxconns 1000
```

Related Commands

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

maxconns (server farm)

To limit the number of active connections to the real server, use the **maxconns** command in SLB server farm configuration mode. To restore the default of 4294967295, use the **no** form of this command.

maxconns *maximum-number* [**sticky-override**]

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active connections on the real server. Valid values range from 1 to 4294967295. The default is 4294967295.
sticky-override	(Optional) Allow sticky load balancing to exceed *maximum-number* for this real server.

Defaults

The default maximum number of simultaneous active connections on the real server is 4294967295.

Command Modes

SLB server farm 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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(18)E	The **sticky-override** keyword was 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.

Examples

The following example limits the real server to a maximum of 1000 simultaneous active connections:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# maxconns 1000
```

Related Commands

Command	Description
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 severfarms	Displays information about the server farm configuration.

mls aging slb normal

To configure the aging time for flows, use the **mls aging slb normal** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls aging slb normal *time*

no mls aging slb normal *time*

Syntax Description

time	Idle time, in milliseconds, before a flow is aged. The valid range is 1 milliseconds to 10000 milliseconds. The default setting is 2000 milliseconds. **Note** Heavier-than-normal loads can age flows more aggressively than this time.

Defaults

The default aging idle time is 2000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(8)E	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

This command is supported for Catalyst 6000 family switches only.

Examples

The following example sets the idle time to 4000 milliseconds:

```
Router(config)# mls aging slb normal 4000
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall farm and initiates firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.
mls aging slb process	Controls how often the aging process runs.

mls aging slb process

To control how often the aging process runs, use the **mls aging slb process** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls aging slb process *time*

no mls aging slb process *time*

Syntax Description

time	Aging process interval, in milliseconds. The valid range is 1 millisecond to 10000 milliseconds. The default setting is 2000 seconds.

Defaults

The default aging process interval is 2000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(8)E	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

This command is supported for Catalyst 6000 family switches only.

Examples

The following example sets the aging process interval to 4000 milliseconds:

```
Router(config)# mls aging slb process 4000
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall farm and initiates firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.
mls aging slb normal	Configures the aging time for flows.

mls ip install-threshold

To install the configured ACL thresholds, use the **mls ip install-threshold** command in global configuration mode.

mls ip install-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Defaults

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **mls ip install-threshold** command is active only when you enable the **mls ip reflexive ndr-entry tcam** command.

Examples

This example shows how to install an ACL threshold:

```
Router(config)# mls ip install-threshold 123
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip reflexive ndr-entry tcam

To enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **mls ip reflexive ndr-entry tcam** command in global configuration mode. To disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **no** form of this command.

mls ip reflexive ndr-entry tcam

no mls ip reflexive ndr-entry tcam

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on Cisco 7600 series routers that are configured with a Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When you enter the **mls ip reflexive ndr-entry tcam** command, the reflexive ACL dynamic entries are installed in TCAM instead of in NetFlow.

Examples

This example shows how to enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# mls ip reflexive ndr-entry tcam
```

This example shows how to disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# no mls ip reflexive ndr-entry tcam
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes configured ACL thresholds.
mls ip install-threshold	Installs the configured ACL thresholds.

mls ip slb purge global

To specify protocol-level purging of MLS entries from active TCP and UDP flow packets, use the **mls ip slb purge global** command in global configuration mode. To disable purge throttling, use the **no** form of this command.

mls ip slb purge global

no mls ip slb purge global

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is for protocol-level purging.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)SX	This command was introduced.
12.2(33)SRD2	The command was modified so that the default command no longer appears in the generated configuration.
12.2(33)SXI2	The command was modified so that the default command no longer appears in the generated configuration.
12.2(18)SXF17	The command was modified so that the default command no longer appears in the generated configuration.

Examples

The following example disables purge throttling on TCP and UDP flow packets:

```
Router(config)# no mls ip slb purge global
Router(config)#
```

The following example returns purge throttling on TCP and UDP flow packets to its default setting:

```
Router(config)# mls ip slb purge global
Router(config)#
```

mls ip slb search wildcard

To specify the behavior of IOS Server Load Balancing (IOS SLB) wildcard searches, use the **mls ip slb search wildcard** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls ip slb search {**wildcard** [**pfc** | **rp**] | **icmp**}

no mls ip slb search {**wildcard** [**pfc** | **rp**] | **icmp**}

Syntax Description

wildcard	IOS SLB wildcard searches are to be performed by the Policy Feature Card (PFC). This value is the default setting.
pfc	(Optional) IOS SLB wildcard searches are to be performed by the Policy Feature Card (PFC). This value is the default setting.
rp	(Optional) IOS SLB wildcard searches are to be performed by the route processor.
icmp	Disables ICMP handling by IOS SLB. (Pings to IOS SLB virtual IP addresses are still answered.) Use this command to reduce CPU usage when IOS SLB is configured in locations with a high volume of ICMP flows, such as in the network core. **Note** Use of the **icmp** keyword can result in minor ICMP errors, such as flows returned to the client with no Network Address Translation (NAT).

Defaults

The default setting is for the PFC to perform IOS SLB wildcard searches.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)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 supported for Catalyst 6500 family switches only.

If you configure IOS SLB and either input ACLs or firewall load balancing on the same Catalyst 6500 Family Switch, you can exceed the capacity of the TCAM on the PFC. To correct the problem, use the **mls ip slb search wildcard rp** command to reduce the amount of TCAM space used by IOS SLB. However, be aware that this command can result in a slight increase in route processor utilization.

Examples

The following example limits wildcard searches to the route processor:

```
Router(config)# mls ip slb search wildcard rp
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.

nat

To configure Cisco IOS Server Load Balancing (IOS SLB) Network Address Translation (NAT) and specify a NAT mode, use the **nat** command in SLB server farm configuration mode. To remove a NAT configuration, use the **no** form of this command.

nat {**client** *pool* | **server**}

no nat {**client** | **server**}

Syntax Description

client *pool*	Configures the client address in load-balanced packets using addresses from the client address pool. The pool name must match the *pool* argument from a previous **ip slb natpool** command. This mode is commonly referred to as *directed client NAT*, or simply client NAT.
server	Configures the destination address in load-balanced packets sent to the real server as the address of the real server chosen by the server farm load-balancing algorithm. This mode is commonly referred to as *directed server NAT*, or simply server NAT.

Defaults

No IOS SLB NAT is configured.

Command Modes

SLB server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.1(1)E	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(2)E	The **client** keyword and *pool* 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 **no nat** command is allowed only if the virtual server was removed from service with the **no inservice** command.

Examples

The following example enters server farm configuration mode and configures NAT mode as server address translation on server farm FARM2:

```
Router# ip slb serverfarm FARM2
Router(config-slb-sfarm)# nat server
```

The following example configures the NAT mode on server farm FARM2 to client translation mode and, using the **real** command in server farm configuration mode, configures the real server IP address as 10.3.1.1:

```
Router(config-slb-sfarm)# nat client web-clients
Router(config-slb-sfarm)# real 10.3.1.1
```

Related Commands

Command	Description
ip slb serverfarm	Associates a real server farm with a virtual server.
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 serverfarms	Displays information about the server farm configuration.

object (tracking)

To specify an object for a tracked list, use the **object** command in tracking configuration mode. To remove the object from the tracked list, use the **no** form of this command.

object *object-number* [**not**] [**weight** *weight-number*]

no object *object-number* [**not**] [**weight** *weight-number*]

Syntax Description

object-number	Object in a tracked list of objects. The range is from 1 to 1000.
not	(Optional) Negates the state of an object. **Note** The **not** keyword cannot be used in a weight or percentage threshold list. It can only be used in a Boolean list.
weight *weight-number*	(Optional) Specifies a threshold weight for each object.

Command Default

The object is not included in the tracked list.

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.
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.
15.1(3)T	This command was modified. The valid range of 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 two serial interfaces (objects) that are in tracked list 100. The Boolean "not" negates the state of object 2, resulting in the tracked list regarding object 2 as down when it is up.

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
```

```
Router(config)# track 100 list boolean and
Router(config-track)# object 1
Router(config-track)# object 2 not
```

Related Commands

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

password (DFP agent)

To configure a Dynamic Feedback Protocol (DFP) agent password for Message Digest Algorithm Version 5 (MD5) authentication, use the **password** command in DFP agent configuration mode. To remove the DFP agent password, use the **no** form of this command.

password [**0** | **7**] *password* [*timeout*]

no password

Syntax Description

0	(Optional) Indicates that the password is unencrypted. This is the default setting.
7	(Optional) Indicates that the password is encrypted.
password	Password value for MD5 authentication. **Note** This password must match the password configured on the host agent.
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The valid range is from 0 to 65535. The default is 180.

Defaults

The password encryption default is 0 (unencrypted).
The password timeout default is 180 seconds.

Command Modes

DFP agent configuration (config-dfp)

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The password specified on this command must match the password specified on the DFP manager.

The timeout option allows you to change the password without stopping messages between the DFP agent and its manager. The default value is 180 seconds.

During the timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the agent sends and receives packets only with the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. Setting a longer timeout allows enough time for you to update the password on all agents and servers before the timeout expires. It also prevents mismatches between agents and servers that have begun running the new password and agents, and servers on which you have not yet changed the old password.

If you are running IOS SLB as a DFP manager, and you specify a password on the **ip slb dfp** command in global configuration mode, the password must match the one specified on the **password** command in DFP agent configuration mode in the DFP agent.

Examples

The following example sets the DFP agent password (unencrypted by default) to Password1 and the timeout to 360 seconds:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# password Password1 360
```

Related Commands

Command	Description
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.
replicate casa (firewall farm)	Configures a stateful backup of IOS SLB decision tables to a backup switch.
replicate casa (virtual server)	Configures a stateful backup of IOS SLB decision tables to a backup switch.

peer port

To specify the port to which the IOS SLB KeepAlive Application Protocol (KAL-AP) agent is to connect, use the **peer port** command in SLB Content Application Peering Protocol (CAPP) configuration mode. To restore the default settings, use the **no** form of this command.

peer [*ip-address*] **port** *port*

no peer [*ip-address*] **port** *port*

Syntax Description

ip-address	(Optional) IP address of the peer KAL-AP manager.
port	Content Application Peering Protocol (CAPP) User Datagram Protocol (UDP) port number to which the KAL-AP agent is to connect. Valid port numbers are 1 to 65535.

Defaults

If you do not specify a port, the KAL-AP agent connects to port 5002.

Command Modes

SLB CAPP configuration (config-slb-capp)

Command History

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

Usage Guidelines

Use this command to specify a port number, other than port 5002, to be used by the KAL-AP agent.

You can configure any number of **peer port** commands with the *ip-address* argument, but only one without the *ip-address* argument.

Examples

The following example configures the KAL-AP agent to connect to port number 6000:

```
Router(config-slb-capp)# peer port 6000
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.

peer secret

To enable Message Digest Algorithm Version 5 (MD5) authentication for the IOS SLB KeepAlive Application Protocol (KAL-AP) agent, use the **peer secret** command in SLB Content Application Peering Protocol (CAPP) configuration mode. To disable MD5 authentication, use the **no** form of this command.

peer [*ip-address*] **secret** [*encrypt*] *secret-string*

no peer [*ip-address*] **secret** *secret-string*

Syntax Description

ip-address	(Optional) IP address of the peer KAL-AP.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the KAL-AP client.

Defaults

The KAL-AP agent does not use MD5 authentication with IOS SLB.

Command Modes

SLB CAPP configuration (config-slb-capp)

Command History

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

Usage Guidelines

You can configure any number of **peer secret** commands with the *ip-address* argument, but only one without the *ip-address* argument.

Examples

The following example configures secret string SECRET_STRING for the KAL-AP agent:

```
Router(config-slb-capp)# peer secret SECRET_STRING
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.

platform trace runtime process forwarding-manager module wccp

To enable Forwarding Manager Route Processor and Embedded-Service-Processor trace messages for the Web Cache Communication Protocol (WCCP) process, use the **platform trace runtime process forwarding-manager module wccp** command in global configuration mode. To disable debug messages, use the **no** form of this command.

platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*}

no platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module wccp**

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • **F0**—Embedded Service Processor slot 0 • **R0**—Route Processor slot 0 • **F1**—Embedded Service Processor slot 1 • **R1**—Route Processor slot 1
bay	Chassis bay to configure. Valid options are: • **0** • **1**
level *level*	Selects the trace level. The trace level determines how much information about a module should be stored in the trace buffer or file. Valid options are: • **debug**—Provides debug-level output. • **emergency**—Provides information about an issue that makes the system unusable. • **error**—Provides information about a system error. • **info**—Informational purposes only. • **noise**—All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. • **notice**—Provides information regarding a significant issue, but the router is still working normally. • **verbose**—All possible tracing messages are sent. • **warning**—Provides information about a system warning.

Command Default

The default tracing level for every module on the Cisco ASR 1000 Series Routers is notice.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines Trace level settings are leveled: every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3 (error) ensures that the trace file contains all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) ensures that all trace output for the specific module is included in that trace file.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

When setting trace levels, it is also important to remember that the setting is not done in a configuration mode, so trace level settings are returned to their defaults after every router reload.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to the debug level or higher should be done with discretion.

Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples In the following example, the trace level for the WCCP module in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info):

```
Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module
wccp level info
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

port (custom UDP probe)

To specify the port to which a custom User Datagram Protocol (UDP) probe is to connect, use the **port** command in custom UDP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	UDP port number to which the custom UDP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real (server farm)** command for more details.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	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 configures a custom UDP probe named PROBE6, enters custom UDP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE6 custom UDP
Router(config-slb-probe)# port 8
```

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.
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 probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

port (DFP agent)

To define the port number to be used by the Dynamic Feedback Protocol (DFP) manager to connect to the DFP agent, use the **port** command in DFP agent configuration mode. To disable the port number definition and remove existing connections, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Port number used by a DFP manager to connect to a DFP agent. The valid range is from 1 to 65535.

Defaults

No port number is defined.

Command Modes

DFP agent configuration (config-dfp)

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example, the DFP manager is enabled to connect to the DFP agent using port number 2221:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# port 2221
```

Related Commands

Command	Description
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.

port (HTTP probe)

To specify the port to which an HTTP probe is to connect, use the **port** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	TCP or User Datagram Protocol (UDP) port number to which the HTTP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real** (server farm) command for more details.

Command Modes

HTTP 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

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# port 8
```

Related Commands

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

port (TCP probe)

To specify the port to which a TCP probe is to connect, use the **port** command in TCP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	TCP port number to which the TCP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real** (server farm) command for more details.

Command Modes

TCP 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

The following example configures a TCP probe named PROBE5, enters TCP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# port 8
```

Related Commands

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

predictor

To specify the load-balancing algorithm for selecting a real server in the server farm, use the **predictor** command in SLB server farm configuration mode. To restore the default load-balancing algorithm of weighted round robin, use the **no** form of this command.

predictor [**roundrobin** | **leastconns** | **route-map** *mapname*]

no predictor

Syntax Description

roundrobin	(Optional) Uses the weighted round robin algorithm for selecting the real server to handle the next new connection for the server farm. See the "Weighted Round Robin" section for a detailed description of this algorithm. This algorithm is the default value. RADIUS load balancing requires the weighted round robin algorithm. General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled requires the weighted round robin algorithm. The Home Agent Director requires the weighted round robin algorithm.
leastconns	(Optional) Uses the weighted least connections algorithm for selecting the real server to handle the next new connection for this server farm. See the "Weighted Least Connections" section for a detailed description of this algorithm.
route-map *mapname*	(Optional) Uses IOS policy-based routing (PBR) for selecting the real server to handle the next new connection for this server farm. The *mapname* argument identifies the IOS PBR route map to be used. See the "Route Map" section for a detailed description of this algorithm. The route map algorithm is supported only for RADIUS load balancing accelerated data plane forwarding.

Defaults

If you do not enter a **predictor** command, or if you enter the **predictor** command without specifying a load-balancing algorithm, the weighted round robin algorithm is used.

Command Modes

SLB server farm configuration (config-slb-sfarm)

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.

Release	Modification
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.
12.2(33)SRC	The **route-map** keyword and *mapname* argument were added.

Usage Guidelines

RADIUS load balancing requires the weighted round robin algorithm.

The route map algorithm is supported only for RADIUS load balancing accelerated data plane forwarding. When you specify the **predictor route-map** command, no further commands in SLB server farm configuration mode or real server configuration mode are allowed.

GPRS load balancing without GTP cause code inspection enabled requires the weighted round robin algorithm. A server farm that uses weighted least connections can be bound to a virtual server providing GPRS load balancing without GTP cause code inspection enabled, but you cannot place the virtual server INSERVICE. If you try to do so, Cisco IOS SLB) issues an error message.

The Home Agent Director requires the weighted round robin algorithm. A server farm that uses weighted least connections can be bound to a Home Agent Director virtual server, but you cannot place the virtual server INSERVICE. If you try to do so, Cisco IOS SLB issues an error message.

Examples

The following example specifies the weighted least connections algorithm:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# predictor leastconns
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farm configuration.
weight (server farm)	Specifies the real server's capacity, relative to other real servers in the server farm.

predictor hash address (firewall farm)

To specify the load-balancing algorithm for selecting a firewall in the firewall farm, use the **predictor hash address** command in firewall farm configuration mode. To restore the default load-balancing algorithm, use the **no** form of this command.

predictor hash address [**port**]

no predictor

Syntax Description

port	(Optional) Uses the source and destination TCP or User Datagram Protocol (UDP) port numbers, in addition to the source and destination IP addresses, when selecting a firewall.

Defaults

IOS Server Load Balancing (IOS SLB) uses the source and destination IP addresses when selecting a firewall.

Command Modes

Firewall farm configuration (config-slb-fw)

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

The following example specifies that source and destination IP addresses are to be used when selecting a firewall:

```
Router(config)# ip slb firewall FIRE1
Router(config-slb-fw)# predictor hash address
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.
weight (firewall farm real server)	Specifies the firewall's capacity, relative to other firewalls in the firewall farm.

probe (firewall farm real server)

To associate a probe with a firewall farm, use the **probe** command in firewall farm real server configuration mode. To remove the association, use the **no** form of this command.

probe *probe*

no probe *probe*

Syntax Description

probe	Name of the probe to associate with this firewall farm.

Defaults

No probe is associated with a firewall farm.

Command Modes

Firewall farm real server configuration (config-slb-fw-real)

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

You can configure more than one probe for each firewall in a firewall farm.

If you configure probes in your network, you must also do one of the following:

- Configure the **exclude** keyword on the **client** command on the virtual server, to exclude connections initiated by the client IP address from the load-balancing scheme.
- Configure IP addresses on the IOS Server Load Balancing (IOS SLB) device that are Layer 3-adjacent to the real servers used by the virtual server.

Examples

The following example associates probe FireProbe with server farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw-real)# probe FireProbe
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the server farm configuration.

probe (server farm)

To associate a probe with a server farm, use the **probe** command in server farm configuration mode. To remove the association, use the **no** form of this command.

probe *probe*

no probe *probe*

Syntax Description

probe	Name of the probe to associate with this server farm.

Defaults

No probe is associated with a server farm.

Command Modes

Server farm configuration (config-slb-sfarm)

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

You can configure more than one probe for each server farm.

If you configure probes in your network, you must also do one of the following:

- Configure the **exclude** keyword on the **client** command on the virtual server, to exclude connections initiated by the client IP address from the load-balancing scheme.
- Configure IP addresses on the IOS Server Load Balancing (IOS SLB) device that are Layer 3-adjacent to the real servers used by the virtual server.

Examples

The following example associates probe PROBE1 with server farm PUBLIC:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# probe PROBE1
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farm configuration.

protocol datagram

To enter firewall farm datagram protocol configuration mode, use the **protocol datagram** command in firewall farm configuration mode.

protocol datagram

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(11b)E	This command was introduced, replacing the **udp** command.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E, replacing the **protocol udp** command.
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

Firewall farm datagram protocol configuration applies to the Encapsulation Security Payload (ESP), Generic Routing Encapsulation (GRE), IP in IP encapsulation, and User Datagram Protocol (UDP) protocols.

Examples

The following example enters firewall farm datagram protocol configuration mode:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

protocol tcp

To enter firewall farm TCP protocol configuration mode, use the **protocol tcp** command in firewall farm configuration mode.

protocol tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(11b)E	This command was introduced, replacing the **tcp** command.
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

The following example enters firewall farm TCP protocol configuration mode:

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

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

purge connection

To enable IOS SLB firewall load balancing to send purge requests for connections, use the **purge connection** command in firewall farm configuration mode. To prevent the sending of purge requests, use the **no** form of this command.

purge connection

no purge connection

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB firewall load balancing sends purge requests for connections.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

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

Usage Guidelines

By default, IOS SLB firewall load balancing sends purge requests for connections. However, if a large number of purge requests are sent, the CPU might be impacted. To prevent this problem, use the **no** form of this command to prevent the sending of purge requests.

Examples

The following example prevents the sending of purge requests for connections:

```
Router(config-slb-fw)# no purge connection
```

Related Commands

mls ip slb purge global	Specifies protocol-level purging of MLS entries from active TCP and UDP flow packets.
purge sticky	TBD

purge radius framed-ip acct on-off

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, use the **purge radius framed-ip acct on-off** command in virtual server configuration mode. To disable this behavior, use the **no** form of this command.

purge radius framed-ip acct on-off

no purge radius framed-ip acct on-off

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB purges entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting ON or OFF message.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(11b)E	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 prevents IOS SLB from purging entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting ON or OFF message:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no purge radius framed-ip acct on-off
```

Related Commands

Command	Description
sticky (virtual server)	Assigns all connections from a client to the same real server.

purge radius framed-ip acct stop

To enable IOS Server Load Balancing to purge entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message, use the **purge radius framed-ip acct stop** in virtual server configuration mode. To disable this behavior, use the **no** form of this command.

purge radius framed-ip acct stop {*attribute-number* | **26** | **vsa** {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}

no purge radius framed-ip acct stop {*attribute-number* | **26** | **vsa** {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}

Syntax Description

attribute-number	RADIUS attribute number.
26	RADIUS attribute number 26.
vsa	Vendor-specific attribute number.
vendor-ID	Vendor ID.
3gpp	Third Generation Partnership Project (3GPP) vendor ID.
3gpp2	Third Generation Partnership Project 2 (3GPP2) vendor ID.
sub-attribute-number	Sub-attribute number.

Defaults

IOS SLB purges entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	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 prevents IOS SLB from purging entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no purge radius framed-ip acct stop 44
```

Related Commands

Command	Description
sticky (virtual server)	Assigns all connections from a client to the same real server.

purge sticky

To enable IOS SLB firewall load balancing to send purge requests for sticky connections when the sticky timer expires, use the **purge sticky** command in firewall farm configuration mode. To prevent the sending of purge requests when the timer expires, use the **no** form of this command.

purge sticky

no purge sticky

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB firewall load balancing sends purge requests when the sticky timer expires.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

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

Usage Guidelines

By default, IOS SLB firewall load balancing sends purge requests for sticky connections when the sticky timer expires. However, large volumes of purge requests can impact the CPU. To prevent this problem, use the **no** form of this command to prevent the sending of purge requests when the sticky timer expires.

To configure a sticky timer for IOS SLB firewall load balancing, use the **sticky** command in either firewall farm datagram protocol or firewall farm TCP protocol configuration mode.

Examples

The following example prevents the sending of purge requests for sticky connections:

```
Router(config-slb-fw)# no purge sticky
```

Related Commands

mls ip slb purge global	Specifies protocol-level purging of MLS entries from active TCP and UDP flow packets.
purge connection	Enables IOS SLB firewall load balancing to send purge requests for connections.
sticky (firewall farm datagram protocol)	Assigns all connections from a client to the same firewall.
sticky (firewall farm TCP protocol)	Assigns all connections from a client to the same firewall.

radius acct local-ack key

To enable a RADIUS virtual server to acknowledge RADIUS accounting messages, use the **radius acct local-ack key** command in SLB virtual server configuration mode. To restore the default behavior, use the **no** form of this command.

radius acct local-ack key [*encrypt*] *secret-string*

no radius acct local-ack key [*encrypt*] *secret-string*

Syntax Description

encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).

Defaults

By default, this command is not enabled. When this command is enabled, the RADIUS load balancing device, not the real server, acknowledges RADIUS accounting messages.
If you configure this command but you do not specify the **7** keyword, the *secret-string* is stored in the plain text.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

Configure this command only on a RADIUS virtual server.

Examples

The following example shows how to enable RADIUS virtual server PUBLIC_RADIUS to acknowledge RADIUS accounting messages with key SECRET_PASSWORD.

```
Router(config)# ip slb vserver PUBLIC_RADIUS
Router(config-slb-vserver)# radius acct local-ack key SECRET_PASSWORD
```

Related Commands

Command	Description
ip slb serverfarm	Identifies a server farm and enters server farm configuration mode.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

radius inject acct key

To configure a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and to enable Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation, use the **radius inject acct key** command in SLB virtual server configuration mode. To disable VSA correlation on this virtual server, use the **no** form of this command.

radius inject acct *group-number* **key** [*encrypt*] *secret-string*

no radius inject acct *group-number* **key** *secret-string*

Syntax Description

group-number	VSA correlation group number to be used for VSA correlation in the RADIUS Accounting-Start packets.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded.

Defaults

VSA correlation is disabled on this virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation accounting virtual servers.

Examples

The following example configures VSA correlation group 1 and configures plain text secret string SECRET_STRING for VSA correlation:

```
Router(config-slb-vserver)# radius inject acct 1 key 0 SECRET_STRING
```

Related Commands

Command	Description
radius inject auth	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.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

radius inject auth

To configure a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and to specify whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames, use the **radius inject auth** command in SLB virtual server configuration mode. To disable VSA correlation on this virtual server, use the **no** form of this command.

radius inject auth *group-number* {**calling-station-id** | **username**}

no radius inject auth *group-number* {**calling-station-id** | **username**}

Syntax Description

group-number	VSA correlation group number.
calling-station-id	Specifies that IOS SLB is to create VSA correlation entries based on the RADIUS calling station ID attribute in the RADIUS payload when RADIUS Access-Request messages are exchanged.
username	Specifies that IOS SLB is to create VSA correlation entries based on the RADIUS username attribute in the RADIUS payload when RADIUS Access-Request messages are exchanged.

Defaults

VSA correlation is disabled on this virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

For a given authentication virtual server, you can configure a single **radius inject auth** *group-number* **calling-station-id** command or a single **radius inject auth** *group-number* **username** command, but not both.

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example configures VSA correlation group 1 and specifies that IOS SLB is to create VSA correlation entries based on the RADIUS calling station ID attribute:

```
Router(config-slb-vserver)# radius inject auth 1 calling-station-id
```

Related Commands

Command	Description
calling-station-id	Configures an ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload.

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
username	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

radius inject auth timer

To configure a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, use the **radius inject auth timer** command in SLB virtual server configuration mode. To delete the VSA correlation timer from the configuration, use the **no** form of this command.

radius inject auth timer *seconds*

no radius inject auth timer

Syntax Description

seconds	Time, in seconds, that IOS SLB maintains an entry in the VSA correlation database. Valid range is 1 to 255.

Defaults

No VSA correlation timer is configured for the authentication virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example configures a VSA correlation timer of 45 seconds:

```
Router(config-slb-vserver)# radius inject auth timer 45
```

Related Commands

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth	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.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

radius inject auth vsa

To buffer vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, use the **radius inject auth vsa** command in SLB virtual server configuration mode.

radius inject auth vsa *vendor-id*

Syntax Description

vendor-id	VSA to be buffered: • **cisco**—Only the Cisco VSA can be buffered at this time.

Defaults

VSAs are not buffered.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example buffers the Cisco VSA:

```
Router(config-slb-vserver)# radius inject auth vsa cisco
```

Related Commands

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth	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.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

rate

To specify the maximum number of connections allowed for a real server in a server farm, use the **rate** command in real server configuration mode. To remove the rate limit, use the **no** form of this command.

rate *maximum-rate* [**burst** *burst-rate*]

no rate

Syntax Description

maximum-rate	Maximum number of connections allowed for the real server. Valid values range from 1 to 4294967295.
burst *burst-rate*	(Optional) Maximum connection burst rate allowed for the real server. Configure a burst rate if you expect the real server to receive connection requests at random intervals. Valid values range from (*maximum-rate*/10) + 1 to *maximum-rate*. The default burst rate is (*maximum-rate*/10) connections per second. We recommend that you specify a burst rate of at least (*maximum-rate*/4). For example, if *maximum-rate* is set to 3212, the valid range is 322 to 3212; the default burst rate is (3212/10), or 321 connections per second; and we recommend a burst rate of at least (3212/4), or 803 connections per second.

Defaults

There is no limit on the number of connection allowed for the real server.
If you do not configure a burst rate, the default burst rate is (*maximum-rate*/10) connections per second.

Command Modes

Real server configuration (config-slb-real)

Command History

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

Usage Guidelines

The **rate** command is valid only for real servers in server farms. It is not valid for real servers in firewall farms.

If the rate limit for a real server is exceeded, and a new connection request is received, IOS SLB assigns the new connection request to the next **rate**-configured real server in the server farm's queue. If no other **rate**-configured real server is available in the server farm, IOS SLB drops the connection request.

The rate limit also applies to sticky connections. That is, if the rate limit for a real server is exceeded, and a new sticky connection request is received, IOS SLB drops the sticky connection request.

IOS SLB uses slow start even if a real server has a rate limit configured.

Examples

The following example specifies that up to 100 connections per second are allowed for the real server in a server farm, with a burst rate of 25 burst connections per second:

```
Router(config-slb-real)# rate 100 burst 25
```

real (firewall farm)

To identify a firewall as a member of a firewall farm and enter real server configuration mode, use the **real** command in firewall farm configuration mode. To remove the firewall from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

real *ip-address*

no real *ip-address*

Syntax Description

ip-address	Real server IP address.

Defaults

No firewall is identified as a member of a firewall farm.

Command Modes

Firewall farm configuration (config-slb-fw)

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

A firewall farm comprises a number of firewalls. The firewalls are the physical devices that provide the firewall load-balanced services.

Examples

The following example identifies a firewall as a member of firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# real 10.1.1.1
```

Related Commands

Command	Description
inservice (firewall farm real server)	Enables the firewall for use by IOS SLB.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

real (server farm)

To identify a real server as a member of a server farm and enter real server configuration mode, use the **real** command in SLB server farm configuration mode. To remove the real server from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

real *ipv4-address* [**ipv6** *ipv6-address*] [*port*]

no real *ipv4-address* [**ipv6** *ipv6-address*] [*port*]

Syntax Description

ipv4-address	Real server IPv4 address.
ipv6 *ipv6-address*	(Optional) For dual-stack, real server IPv6 address.
port	(Optional) Port translation for the server. Valid values range from 1 to 65535.

Command Default

No real server is identified as a member of a server farm.

Command Modes

SLB server farm configuration (config-slb-sfarm)

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(2)E	The *port* argument was 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.
15.0(1)S	The **ipv6** keyword and *ipv6-address* argument were added.

Usage Guidelines

A server farm comprises a number of real servers. The real servers are the physical devices that provide the load-balanced services.

In general packet radio service (GPRS) load balancing, this command identifies a gateway GPRS support node (GGSN) that is a member of the server farm. Also, remember that the Cisco GGSN IP addresses are virtual template IP addresses, not real interface IP addresses.

IOS SLB supports GPRS Tunneling Protocol (GTP) v0, v1, and v2 real servers. A GTP v2 real server can be either a Packet Data Network Gateway (PGW) or a serving gateway (SGW).

- A GTP v2 PGW can also manage GTP v0 and v1 requests.
- A GTP v2 SGW cannot manage GTP v0 or v1 requests.
- A GTP v0 or v1 real server cannot manage GTP v2 requests. Therefore, you must configure separate virtual servers for GTPv2 real servers and GTP v0 or v1 real servers.

IOS SLB supports dual-stack addresses for GTP load balancing only. To support dual-stack addresses, you must configure the real server as a dual-stack real server, with the IPv4 and IPv6 addresses, using this command.

In Virtual Private Network (VPN) server load balancing, this command identifies a real server acting as a VPN terminator.

Examples

The following example identifies a real server as a member of the server farm:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.1.1.1
```

The following example identifies a dual-stack real server as a member of the server farm:

```
Router(config)# ip slb serverfarm DUAL-PUBLIC
Router(config-slb-sfarm)# real 10.1.1.1 ipv6 12AB:0000:0000:CD31:0000:0000:0000:0000/64
```

Related Commands

Command	Description
inservice (server farm real server)	Enables the real server for use by IOS SLB.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

real (static NAT)

To configure one or more real servers to use static Network Address Translation (NAT), use the **real** command in static NAT configuration mode. To restore the default behavior, use the **no** form of this command.

real *ip-address* [*port*]

no real *ip-address* [*port*]

Syntax Description

ip-address	IP address of the real server that is to use static NAT.
port	(Optional) Layer 4 source port number, used by IOS Server Load Balancing (IOS SLB) to differentiate between User Datagram Protocol (UDP) responses from the real server and connections initiated by the real server.

Defaults

No real server is configured to use static NAT.

Command Modes

Static NAT configuration (config-slb-static)

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.

Usage Guidelines

If no port number is specified, IOS SLB uses static NAT for all packets outbound from the real server.

Examples

The following example configures real server 10.1.1.3 to use static NAT:

```
Router(config)# ip slb static nat
Router(config-slb-static)# real 10.1.1.3
```

Related Commands

Command	Description
ip slb static	Configures a real server's NAT behavior and enters static NAT configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb static	Displays information about the static NAT configuration.

reassign

To specify 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, use the **reassign** command in SLB real server configuration mode. To restore the default reassignment threshold, use the **no** form of this command.

reassign *threshold*

no reassign

Syntax Description

threshold	Number of unacknowledged TCP SYNs (or Create PDP requests, in general packet radio service [GPRS] load balancing) that are directed to a real server before the connection is reassigned to a different real server. An unacknowledged SYN is one for which no SYN or ACKnowledgment (ACK) is detected before the next SYN arrives from the client. IOS Server Load Balancing (IOS SLB) allows 30 seconds for the connection to be established or for a new SYN to be received. If neither of these occurs within that time, the connection is removed from the IOS SLB database. The 30-second timer is restarted for each SYN as long as the number of connection reassignments specified in the **faildetect numconns (real server)** command is not exceeded. See the **faildetect numconns (real server)** command for more information. Valid threshold values range from one 1 to 4. The default value is 3.

Defaults

The default threshold value is 3.

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 general packet radio service (GPRS) load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Cisco 7600 series routers that are configured with a Supervisor Engine 720.
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 not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

IOS SLB does not reassign sticky connections if either of the following conditions is true:

- The real server is not OPERATIONAL or MAXCONNS_THROTTLED.
- The connection is the first for this sticky connection.

In GPRS load balancing, this command specifies the number of consecutive unacknowledged Create PDP requests (not TCP SYNs) that are directed to a gateway GPRS support node (GGSN) before the connection is reassigned to a different GGSN. You must specify a reassign threshold less than the N3-REQUESTS counter value of the serving GRPS support node (SGSN).

Examples

The following example shows how to set the threshold of unacknowledged SYNs to 2:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# reassign 2
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the IOS SLB feature.
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.

replicate casa (firewall farm)

To configure a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch, use the **replicate casa** command in firewall farm configuration mode. To remove a this configuration, use the **no** form of this command.

replicate casa *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string* [*timeout*]]

no replicate casa *listen-ip remote-ip port*

Syntax Description

listen-ip	Listening IP address for state exchange messages that are advertised.
remote-ip	Destination IP address for all state exchange signals.
port	TCP or User Datagram Protocol (UDP) port number or port name for all state exchange signals.
interval	(Optional) Maximum replication delivery interval from 1 to 300 seconds. The default value is 10 seconds. **Note** While IOS SLB does accept the *interval* argument, the **replicate interval** command is the preferred means for setting the replication delivery interval. In fact, if you set the replication delivery interval using the *interval* argument, IOS SLB writes it into the configuration as a **replicate interval** command.
password	(Optional) Specifies the password for Message Digest Algorithm Version 5 (MD5) authentication.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The default value is 180 seconds.

Defaults

The default interval is 10 seconds.
The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds.

Command Modes

Firewall farm configuration (config-slb-fw)

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 *timeout* option allows you to change the password without stopping messages between the backup and primary Layer 3 switches. The default value is 180 seconds.

During the timeout, the backup sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the backup sends and receives packets only with the new password.

When setting a new password timeout, remember the following considerations:

- If you are configuring a new backup, set the timeout to 0 (send packets with the new password immediately). This configuration prevents password mismatches between the new backup and its primary.
- If you are changing the password for an existing backup, set a longer timeout to allow enough time for you to update the password on the primary before the timeout expires. Setting a longer timeout also prevents mismatches between the backup and primary.

If you configure this command but you do not specify the **7** keyword, the secret-string is stored in the plain text.

Examples

The following example configures a stateful backup Layer-3 switch with a listening IP address of 10.10.10.11 and a remote IP address of 10.10.11.12 over HTTP port 4231:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb replicate	Displays the configuration of IO SLB IP replication.

replicate casa (virtual server)

To configure a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch, use the **replicate casa** command in virtual server configuration mode. To remove this configuration, use the **no** form of this command.

replicate casa *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string* [*timeout*]]

no replicate casa *listen-ip remote-ip port*

Syntax Description

listen-ip	Listening IP address for state exchange messages that are advertised.
remote-ip	Destination IP address for all state exchange signals.
port	TCP or User Datagram Protocol (UDP) port number or port name for all state exchange signals.
interval	(Optional) Maximum replication delivery interval from 1 to 300 seconds. The default value is 10 seconds. **Note** While IOS SLB does accept the *interval* argument, the **replicate interval** command is the preferred means for setting the replication delivery interval. In fact, if you set the replication delivery interval using the *interval* argument, IOS SLB writes it into the configuration as a **replicate interval** command.
password	(Optional) Specifies the password for Message Digest Algorithm Version 5 (MD5) authentication.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The default value is 180 seconds.

Defaults

The default interval is 10 seconds.
The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(3a)E	The **0** and **7** keywords 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 *timeout* option allows you to change the password without stopping messages between the backup and primary Layer 3 switches. The default value is 180 seconds.

During the timeout, the backup sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the backup sends and receives packets only with the new password.

When setting a new password timeout, remember the following considerations:

- If you are configuring a new backup, set the timeout to 0 (send packets with the new password immediately). This configuration prevents password mismatches between the new backup and its primary.
- If you are changing the password for an existing backup, set a longer timeout to allow enough time for you to update the password on the primary before the timeout expires. Setting a longer timeout also prevents mismatches between the backup and primary.

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate casa** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate casa** command in virtual server configuration mode.

If you configure this command but you do not specify the **7** keyword, the secret-string is stored in the plain text.

Examples

The following example configures a stateful backup Layer-3 switch with a listening IP address of 10.10.10.11 and a remote IP address of 10.10.11.12 over HTTP port 4231:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate casa 10.10.10.11 10.10.11.12 4231
```

Related Commands

Command	Description
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vserver	Displays information about the virtual servers defined to IOS SLB.

replicate interval (firewall farm)

To set the replication delivery interval for an IOS Server Load Balancing (IOS SLB) firewall farm, use the **replicate interval** command in firewall farm configuration mode. To restore the default interval, use the **no** form of this command.

replicate interval *interval*

no replicate interval

Syntax Description

interval	Maximum replication delivery interval, in seconds. Replication updates are sent to the peer device (CASA or slave) when the interval expires, or when the send buffer (1500 bytes) is full. The valid range is 1 to 300 seconds. The default value is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.2(14)ZA5	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

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate interval** command in firewall farm configuration mode.

The Home Agent Director does not support the **replicate interval** command in firewall farm configuration mode.

Examples

The following example configures a replication interval of 20 seconds:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate interval 20
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication.
replicate casa (firewall farm)	Configures a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch
replicate slave (firewall farm)	Enables stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) firewall farm.
show ip slb replicate	Displays the configuration of IOS Server Load Balancing (IOS SLB) IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

replicate interval (virtual server)

To set the replication delivery interval for an IOS Server Load Balancing (IOS SLB) virtual server, use the **replicate interval** command in virtual server configuration mode. To restore the default interval, use the **no** form of this command.

replicate interval *interval*

no replicate interval

Syntax Description

interval	Maximum replication delivery interval, in seconds. Replication updates are sent to the peer device (CASA or slave) when the interval expires, or when the send buffer (1500 bytes) is full. The valid range is 1 to 300 seconds. The default value is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	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

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate interval** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate interval** command in virtual server configuration mode.

Examples

The following example configures a replication interval of 20 seconds:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate interval 20
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication.
replicate casa (virtual server)	Configures a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch
replicate slave (virtual server)	Enables stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) virtual server.
show ip slb replicate	Displays the configuration of IOS Server Load Balancing (IOS SLB) IP replication.
show ip slb vserver	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

replicate slave (firewall farm)

To enable stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) firewall farm, if the slave device is present, use the **replicate slave** command in firewall farm configuration mode. To disable stateful backup of redundant route processors, use the **no** form of this command.

replicate slave

no replicate slave

Syntax Description

This command has no arguments or keywords.

Defaults

Stateful backup of redundant route processors is disabled.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.2(14)ZA5	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

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate slave** command in firewall farm configuration mode.

The Home Agent Director does not support the **replicate slave** command in firewall farm configuration mode.

Examples

The following example enables stateful backup of redundant route processors:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate slave
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS SLB slave replication.
replicate casa (firewall farm)	Configures a stateful backup of IOS SLB decision tables to a backup switch
replicate interval (firewall farm)	Sets the replication delivery interval for an IOS SLB firewall farm.
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

replicate slave (virtual server)

To enable stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) virtual server, if the slave device is present, use the **replicate slave** command in virtual server configuration mode. To disable stateful backup of redundant route processors, use the **no** form of this command.

replicate slave

no replicate slave

Syntax Description

This command has no arguments or keywords.

Defaults

Stateful backup of redundant route processors is disabled.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	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

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate slave** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate slave** command in virtual server configuration mode.

If you are using a single Supervisor with **replicate slave** configured, you might receive out-of-sync messages on the Supervisor.

Examples

The following example enables stateful backup of redundant route processors:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate slave
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS SLB slave replication.
replicate casa (virtual server)	Configures a stateful backup of IOS SLB decision tables to a backup switch

Command	Description
replicate interval (virtual server)	Sets the replication delivery interval for an IOS SLB virtual server.
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

request (custom UDP probe)

To define the payload of the User Datagram Protocol (UDP) request packet to be sent by a custom UDP probe, use the **request** command in custom UDP probe configuration mode.

request data {*start-byte* | **continue**} *hex-data-string*

Syntax Description

data *start-byte*	Identifies the payload offset at which the *hex-data-string* is to be placed into the packet.
data continue	String of characters represented by the *hex-data-string* argument is to be placed after the last defined byte in the request packet.
hex-data-string	Payload of the UDP request packet, up to 100 bytes of data in hexadecimal format.

Defaults

The payload of the UDP request packet is not defined.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	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

You can enter more than one **request** command, to specify the entire UDP payload.

Examples

The following example generates custom UDP probe PROBE6, with the specified 119-byte UDP payload.

```
Router(config)# ip slb probe PROBE6 custom UDP
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
Router(config-slb-probe)# request data 20 01 07 63 68 72 69 73 28 06 00 00 00 01 2C 0A 30
30 30 30 30
Router(config-slb-probe)# request data 40 30 30 42 07 06 00 00 00 07 1E 10 63 75 66 66 2E
63 69 73 63
Router(config-slb-probe)# request data 60 6F 2E 63 6F 6D 1F 0C 39 31 39 33 39 32 39 31 36
39 08 06 0A
Router(config-slb-probe)# request data 80 0A 01 01 2D 06 00 00 00 01 3D 06 00 00 00 05 05
06 00 00 00
Router(config-slb-probe)# request data 100 00 06 06 00 00 00 02 04 06 0A 0A 18 0A 29 06 00
00 00 00
```

Related Commands

Command	Description
ip slb probe custom udp	Configures the IOS SLB IP probe name.
response	Defines the data string to match against custom UDP probe response packets.
show ip slb probe	Displays information about an IOS SLB probe.

request (HTTP probe)

To configure an HTTP probe to check the status of the real servers, use the **request** command in HTTP probe configuration mode. To remove a **request** configuration, use the **no** form of this command.

request [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]

no request [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]

Syntax Description

method	(Optional) Configures the way the data is requested from the server.
get	Configures the Get method to request data from the server.
post	Configures the Post method to request data from the server.
head	Configures the header data type to request data from the server.
name *name*	Configures the name string of the data to send to the servers to request data. The character string is limited to 15 characters.
url *path*	(Optional) Configures the path from the server.

Defaults

No HTTP probe is configured to check the status of the real servers.

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 **request** command configures the Cisco IOS Server Load Balancing (Cisco IOS SLB) HTTP probe method used to receive data from the server. Only one Cisco IOS SLB HTTP probe can be configured for each server farm.

If no values are configured following the **method** keyword, the default is Get.

If no URL path is set to the server, the default is /.

Examples

The following example configures an IOS SLB HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures HTTP requests to use the post method and the URL /probe.cgi?all:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# request method post url /probe.cgi?all
```

Related Commands

Command	Description
ip slb probe http	Configures the Cisco IOS SLB IP probe name.
show ip slb probe	Displays information about an Cisco IOS SLB probe.

response

To define the data string to match against custom User Datagram Protocol (UDP) probe response packets, use the **response** command in custom UDP probe configuration mode.

response *clause-number* **data** *start-byte hex-data-string*

Syntax Description

clause-number	Identifies the response clause that is being modified. Up to 8 response clauses can be specified, on individual **response** commands.
data *start-byte*	Byte in the UDP response packet at which the *hex-data-string* is to be matched.
hex-data-string	Up to 100 bytes of data, in hexadecimal format, that is to be matched against the UDP response packet payload. If the data does not match, the probe fails.

Defaults

The data string to match against custom UDP probe response packets is not defined.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	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

You can enter up to 8 individual response commands, to parse up to 8 non-contiguous bytes of data.

Examples

In the following example, if the 26th and 27th bytes of the response from *PROBE6* are not *FF FF*, and the 44th and 45th bytes are not *DD DD*, the probe fails.

```
Router(config)# ip slb probe PROBE6 custom UDP
Router(config-slb-probe)# response 1 data 26 FF FF
Router(config-slb-probe)# response 2 data 44 DD DD
```

Related Commands

Command	Description
ip slb probe custom udp	Configures the IOS SLB IP probe name.
request (custom UDP probe)	Defines the payload of the UDP request packet to be sent by a custom UDP probe.
show ip slb probe	Displays information about an IOS SLB probe.

retry (real server)

To specify how long to wait before a new connection is attempted to a failed server, use the **retry** command in SLB real server configuration mode. To restore the default retry value, use the **no** form of this command.

retry *retry-value*

no retry

Syntax Description

retry-value	Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted. If the new connection attempt succeeds, the real server is placed in OPERATIONAL state. If the connection attempt fails, the timer is reset, the connection is reassigned, and the process repeats until it is successful or until the server is placed in the OUTOFSERVICE state by the network administrator. Valid values range from 1 to 3600. The default value is 60 seconds. A value of 0 means do not attempt a new connection to the server when it fails.

Defaults

The default retry-value is 60 seconds.

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.
12.2(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

The following example specifies that 120 seconds must elapse after the detection of a server failure before a new connection is attempted:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# retry 120
```

Related Commands

Command	Description
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.