



IP Application Services Commands

aaa accounting vrrs

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use the Virtual Router Redundancy Service (VRRS), use the **aaa accounting vrrs** command in global configuration mode. To disable AAA accounting for VRRS, use the **no** form of this command.

aaa accounting vrrs {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting vrrs {**default** | *list-name*} **start-stop** *method1* [*method2*...]

Syntax Description	default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
	<i>list-name</i>	Character string used to name the list of accounting methods. If no list name is specified, the system uses the default value.
	start-stop	Sends an accounting-on notice. The accounting-on record is sent in the background. The requested user process begins regardless of whether the accounting-on notice is received by the accounting server.
	<i>method1</i> [<i>method2</i> ...]	(Optional) Character string used to name at least one of the accounting methods, tried in the specified sequence.

Command Default AAA accounting is disabled for VRRS

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines Use the **aaa accounting vrrs** command to define a AAA accounting method list. If you define the AAA default accounting method list, you are defining the AAA accounting method list for all the VRRS servers. The default AAA accounting method list is applied to all VRRS groups. To specify a group-specific VRRS method list, use the **accounting method** command in VRRS configuration mode.

Examples The following example shows how to configure VRRP group 1 with the group name “vrrp-name-1” to use VRRS method list vrrs-mlist-1:

```
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
!
Router(config-if)# vrrs vrrp-name-1
Router(config)# accounting mlist vrrs-mlist-1
!
Router(config)# interface gigabitethernet0/2/2
```

```
Router(config-if)# ip address 10.0.1.  
Router(config-if)# vrrp 1 ip 10.1.0.10  
Router(config-if)# vrrp 1 name vrrp-name-1
```

Related Commands

Command	Description
vrrp ip	Enables the VRRP on an interface and identifies the IP address of the virtual router.
vrrp name	Links a VRRS client to a VRRP group.

access (firewall farm)

To route specific flows to a firewall farm, use the **access** command in firewall farm configuration mode. To restore the default settings, use the **no** form of this command.

access [**source** *source-ip netmask* | **destination** *destination-ip netmask* |
inbound {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]

no access [**source** *source-ip netmask* | **destination** *destination-ip netmask* |
inbound {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]

Syntax Description

source	(Optional) Routes flows based on source IP address.
<i>source-ip</i>	(Optional) Source IP address. The default is 0.0.0.0 (all sources).
<i>netmask</i>	(Optional) Source IP network mask. The default is 0.0.0.0 (all source subnets).
destination	(Optional) Routes flows based on destination IP address.
<i>destination-ip</i>	(Optional) Destination IP address. The default is 0.0.0.0 (all destinations).
<i>netmask</i>	(Optional) Destination IP network mask. The default is 0.0.0.0 (all destination subnets).
inbound <i>inbound-interface</i>	(Optional) Indicates that the firewall farm is to accept inbound packets only on the specified inbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the <i>inbound-interface</i> argument.
inbound datagram connection	(Optional) Indicates that IOS SLB is to create connections for inbound traffic as well as outbound traffic.
outbound <i>outbound-interface</i>	(Optional) Indicates that the firewall farm is to accept outbound packets only on the specified outbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the <i>outbound-interface</i> argument.

Defaults

The default source IP address is 0.0.0.0 (routes flows from all sources to this firewall farm).
The default source IP network mask is 0.0.0.0 (routes flows from all source subnets to this firewall farm).
The default destination IP address is 0.0.0.0 (routes flows from all destinations to this firewall farm).
The default destination IP network mask is 0.0.0.0 (routes flows from all destination subnets to this firewall farm).
If you do not specify an inbound interface, the firewall farm accepts inbound packets on all inbound interfaces.
If you do not specify the **inbound datagram connection** option, IOS SLB creates connections only for outbound traffic.
If you do not specify an outbound interface, the firewall farm accepts outbound packets on all outbound interfaces.

Command Modes

Firewall farm configuration (config-slb-fw)

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	The inbound and outbound keywords and <i>inbound-interface</i> and <i>outbound-interface</i> arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The datagram connection keywords were added. The <i>inbound-interface</i> and <i>outbound-interface</i> arguments can be subinterfaces.

Usage Guidelines

You can specify more than one source or destination for each firewall farm. To do so, configure multiple **access** statements, making sure the network masks do not overlap each other.

You can specify up to two inbound interfaces and two outbound interfaces for each firewall farm. To do so, configure multiple **access** statements, keeping the following considerations in mind:

- All inbound and outbound interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).
- All inbound and outbound interfaces must be different from each other.
- You cannot change inbound or outbound interfaces for a firewall farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the firewall farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

By default, IOS SLB firewall load balancing creates connections only for outbound traffic (that is, traffic that arrives through the real server). Inbound traffic uses those same connections to forward the traffic, which can impact the CPU. To enable IOS SLB to create connections for both inbound traffic and outbound traffic, reducing the impact on the CPU, use the **access inbound datagram connection** command.

Examples

The following example routes flows with a destination IP address of 10.1.6.0 to firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
```

Related Commands

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

access (server farm)

To configure an access interface for a server farm, use the **access** command in server farm configuration mode. To disable the access interface, use the **no** form of this command.

access *interface*

no access *interface*

Syntax Description

<i>interface</i>	Interface to be inspected. The server farm will handle outbound flows from real servers only on the specified interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the <i>interface</i> argument.
------------------	--

Defaults

The server farm handles outbound flows from real servers on all interfaces.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The <i>interface</i> argument can be a subinterface.

Usage Guidelines

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two access interfaces for each server farm. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- The access interfaces of primary and backup server farms must be the same.
- You cannot change the interfaces for a server farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the server farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example limits the server farm to handling outbound flows from real servers only on access interface Vlan106:

```
Router(config)# ip slb serverfarm SF1
```

```
Router(config-slb-sfarm)# access Vlan106
```

Related Commands

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

access (virtual server)

To enable framed-IP routing to inspect the ingress interface, use the **access** command in virtual server configuration mode. To disable framed-IP routing, use the **no** form of this command.

access *interface* [**route framed-ip**]

no access *interface* [**route framed-ip**]

Syntax Description

<i>interface</i>	Interface to be inspected. You can specify a subinterface, such as GigabitEthernet7/3.100, for the <i>interface</i> argument.
route framed-ip	(Optional) Routes flows using framed-IP routing.

Defaults

Framed-IP routing cannot inspect the ingress interface.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(12c)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	The command was modified to accept up to two framed-IP access interfaces (specified on separate commands).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The <i>interface</i> argument can be a subinterface.

Usage Guidelines

This command enables framed-IP routing to inspect the ingress interface when routing subscriber traffic. All framed-IP sticky database entries created as a result of RADIUS requests to this virtual server will include the interface in the entry. In addition to matching the source IP address of the traffic with the framed-IP address, the ingress interface must also match this interface when this command is configured.

You can use this command to allow subscriber data packets to be routed to multiple service gateway service farms.

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two framed-IP access interfaces for each virtual server. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- You cannot change the interfaces for a virtual server while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the virtual server in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example enables framed-IP routing to inspect ingress interface Vlan20:

```
Router(config)# ip slb vserver SSG_AUTH  
Router(config-slb-vserver)# access Vlan20 route framed-ip
```

Related Commands

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

accounting delay (VRRS)

To specify a delay time for sending accounting-off messages for the Virtual Router Redundancy Service (VRRS), use the **accounting delay** command in VRRS configuration mode. To return to the default accounting delay value, use the **no** form of this command.

accounting delay *seconds*

no accounting delay

Syntax Description	<i>seconds</i>	Time, in seconds, to wait before sending accounting-off messages. Range is from 1 to 30. The default is 0.
---------------------------	----------------	--

Command Default	Accounting-off messages for VRRS are sent without delay.
------------------------	--

Command Modes	VRRS configuration (config-vrrs)
----------------------	----------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines	Use the accounting delay command to control the timing of sending accounting-off messages for VRRS. This command does not apply to accounting-on messages. If the default is specified, this command is not saved to the running configuration and accounting-off messages are sent immediately when the event occurs. Otherwise, a delay of the configured number of seconds is applied.
-------------------------	--

Examples	The following example shows how to specify a delay time of 10 seconds for sending accounting-off messages for the VRRS:
-----------------	---

```
Router(config)# vrrs vrrp-name-1
Router(config-vrrs)# accounting delay 10
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
accounting method (VRRS)	Enables VRRS accounting for a VRRP group.
attribute list (VRRS)	Specifies additional attributes to include in VRRS accounting-on and accounting-off messages.
vrrs	Enables VRRS and enters VRRS configuration mode.

accounting method (VRRS)

To enable Virtual Router Redundancy Service (VRRS) accounting for a Virtual Router Redundancy Protocol (VRRP) group, use the **accounting method** command in VRRS configuration mode. To specify the default VRRS accounting method list as the target for VRRS accounting, use the **no** form of this command.

accounting method { **default** | *accounting-method-list* }

no accounting method

Syntax Description	default	Enables VRRS accounting for all VRRP groups.
	<i>accounting-method-list</i>	Name of the accounting method list for which VRRS must be enabled.

Command Default The default VRRS accounting method list is used.

Command Modes VRRS Configuration (config-vrrs)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines Configuring the **default** keyword does not save it to the running configuration and the VRRS accounting type default method list is automatically applied to the VRRS group being configured. The **default** keyword also enables VRRS accounting for all VRRP groups.

The valued specified for the *accounting-method-list* argument must match a named list configured by the **aaa accounting vrrs** command. When there is no match, a warning message is displayed. However, the configuration is still saved.

With this approach, you can configure the desired accounting method list using the **aaa accounting vrrs** command without configuring the **accounting method** command again.

Examples The following example shows how to configure VRRS to use the accounting list named METHOD1:

```
Router(config)# vrrs VRRS1
Router(config-vrrs)# accounting method METHOD1
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
accounting delay (VRRS)	Specifies a delay time for sending accounting-off messages for VRRS.
attribute list (VRRS)	Specifies additional attributes to include in VRRS accounting-on and accounting-off messages.

address (custom UDP probe)

To configure an IP address to which to send custom User Datagram Protocol (UDP) probes, use the **address** command in custom UDP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address*] [**routed**]

no address [*ip-address*] [**routed**]

Syntax Description

<i>ip-address</i>	(Optional) Destination IP address that is to respond to the custom UDP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to <i>ip-address</i>.

Defaults

If the custom UDP probe is associated with a firewall farm, you must specify an IP address. If the custom UDP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

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 receive responses from IP address 13.13.13.13:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# address 13.13.13.13
```

Related Commands

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

address (DNS probe)

To configure an IP address to which to send Domain Name System (DNS) probes, use the **address** command in DNS probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

<i>ip-address</i>	(Optional) Destination IP address that is to respond to the DNS probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the DNS probe is associated with a firewall farm, you must specify an IP address.
If the DNS probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	The routed keyword 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.

Examples

The following example configures a DNS probe named PROBE4, enters DNS probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# address 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.

address (HTTP probe)

To configure an IP address to which to send HTTP probes, use the **address** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

<i>ip-address</i>	(Optional) Destination IP address that is to respond to the HTTP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the HTTP probe is associated with a firewall farm, you must specify an IP address.
If the HTTP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.1(12c)E	The routed keyword 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.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

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

address (ping probe)

To configure an IP address to which to send ping probes, use the **address** command in ping probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description	<i>ip-address</i>	(Optional) Destination IP address that is to respond to the ping probe.
	routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults	<p>If the ping probe is associated with a firewall farm, you must specify an IP address.</p> <p>If the ping probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.</p>
-----------------	---

Command Modes	Ping probe configuration (config-slb-probe)
----------------------	---

Command History	Release	Modification
	12.1(3a)E	This command was introduced.
	12.1(12c)E	The routed keyword 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.

Examples	<p>The following example configures a ping probe named PROBE1, enters ping probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:</p>
-----------------	---

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# address 10.1.10.1
```

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

address (TCP probe)

To configure an IP address to which to send TCP probes, use the **address** command in TCP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address*] [**routed**]

no address [*ip-address*] [**routed**]

Syntax Description

<i>ip-address</i>	(Optional) Destination IP address that is to respond to the TCP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the TCP probe is associated with a firewall farm, you must specify an IP address.
If the TCP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

TCP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	The routed keyword 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.

Examples

The following example configures a TCP probe named PROBE5, enters TCP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

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

address (WSP probe)

To configure an IP address to which to send Wireless Session Protocol (WSP) probes, use the **address** command in WSP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

<i>ip-address</i>	(Optional) Destination IP address that is to respond to the WSP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: <ul style="list-style-type: none"> Only one instance of a routed probe per server farm can run at any given time. Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the WSP probe is associated with a firewall farm, you must specify an IP address.
If the WSP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.
In dispatched mode, the *ip-address* argument value is the same as the virtual server IP address. In directed Network Address Translation (NAT) mode, an IP address is unnecessary.

Command Modes

WSP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(5a)E	This command was introduced.
12.1(12c)E	The routed keyword 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.

Examples

The following example configures a WSP probe named PROBE3, enters WSP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE3 wsp
Router(config-slb-probe)# address 10.1.10.1
```

■ address (WSP probe)

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

advertise

To control the installation of a static route to the Null0 interface for a virtual server address, use the **advertise** command in SLB virtual server configuration mode. To prevent the installation of a static route for the virtual server IP address, use the **no** form of this command.

advertise [**active**]

no advertise [**active**]

Syntax Description

active	(Optional) Indicates that the host route is to be advertised only when the virtual IP address is available (that is, when there is at least one real server in OPERATIONAL, DFP_THROTTLED, or MAXCONNS state).
---------------	--

Defaults

The virtual server IP address is advertised. That is, a static route to the Null0 interface is installed for the virtual server IP addresses and it is added to the routing table. If you do not specify the **active** keyword, the host route is advertised regardless of whether the virtual IP address is available.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(7)E	The active keyword 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.

Usage Guidelines

Advertisement of a static route using the routing protocol requires that you configure redistribution of static routes for the routing protocol.

The **advertise** command does not affect virtual servers used for transparent web cache load balancing.

HTTP probes and route health injection require a route to the virtual server. The route is not used, but it must exist to enable the sockets code to verify that the destination can be reached, which in turn is essential for HTTP probes and route health injection to function correctly.

- For HTTP probes, the route can be either a host route (advertised by the virtual server) or a default route (specified using the **ip route 0.0.0.0 0.0.0.0** command, for example). If you specify either the **no advertise** or the **advertise active** command, you must specify a default route.
- For route health injection, the route must be a default route.

HTTP probes and route health injection can both use the same default route; you need not specify two unique default routes.

Examples

The following example prevents advertisement of the virtual server's IP address in routing protocol updates:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# no advertise
```

Related Commands

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

agent

To identify a Dynamic Feedback Protocol (DFP) agent with which the IOS Server Load Balancing (IOS SLB) feature can initiate connections, use the **agent** command in SLB DFP configuration mode. To remove a DFP agent definition from the DFP configuration, use the **no** form of this command.

agent *ip-address* *port* [*timeout* [*retry-count* [*retry-interval*]]]

no agent *ip-address* *port*

Syntax Description

<i>ip-address</i>	Agent IP address.
<i>port</i>	Agent TCP or User Datagram Protocol (UDP) port number.
<i>timeout</i>	(Optional) Time period, in seconds, during which the DFP manager must receive an update from the DFP agent. The valid range is 0 to 65535 seconds. The default is 0 seconds, which means there is no timeout.
<i>retry-count</i>	(Optional) Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. The valid range is 0 to 65535 times. The default is 0 retries, which means there are infinite retries.
<i>retry-interval</i>	(Optional) Interval, in seconds, between retries. The valid range is 1 to 65535 seconds. The default is 180 seconds.

Defaults

The default timeout is 0 seconds (no timeout).
 The default retry count is 0 (infinite retries).
 The default retry interval is 180 seconds.

Command Modes

SLB DFP configuration (config-slb-dfp)

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.

Usage Guidelines

A DFP agent collects status information about the load capability of a server and reports that information to a load manager. The DFP agent may reside on the server, or it may be a separate device that collects and consolidates the information from several servers before reporting to the load manager.

The password specified in the **ip slb dfp** command for the DFP manager must match the password specified in the **password** command for the DFP agent.

You can configure up to 1024 agents.

Examples

The following example sets the DFP password to Password1 (to match the DFP agent's password), sets the timeout to 360 seconds, enters DFP configuration mode, and enables IOS SLB to connect to the DFP agent with IP address 10.1.1.1 and port number 2221:

```
Router(config)# ip slb dfp password Password1 360
Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10
```

Related Commands

Command	Description
ip dfp agent	Identifies a DFP agent subsystem and enters DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and enters DFP configuration mode.

apn

To configure an ASCII regular expression string to be matched against the access point name (APN) for general packet radio service (GPRS) load balancing, use the **apn** command in SLB GTP map configuration mode. To delete the APN string, use the **no** form of this command.

apn *string*

no apn *string*

Syntax Description	<i>string</i>	ASCII regular expression string to be matched against the APN. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the “Understanding Regular Expressions” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> : http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
Defaults	None	
Command Modes	SLB GTP map configuration (config-slb-gtp-map)	
Command History	Release	Modification
	12.2(33)SRB	This command was introduced.
Usage Guidelines	For a given IOS SLB GTP map, you can configure up to 100 apn commands. However, we recommend you configure no more than 10 apn commands per map.	
Examples	The following example specifies that, for IOS SLB GTP map 2, string .cisco* is to be matched against the APN: Router(config)# ip slb map 2 gtp Router(config-slb-gtp-map)# apn cisco*	
Related Commands	Command	Description
	ip slb map	Configures an IOS SLB protocol map and enters SLB map configuration mode.
	show ip slb map	Displays information about IOS SLB protocol maps.

attribute list (VRRS)

To specify additional attributes to include in Virtual Router Redundancy Service (VRRS) accounting-on and accounting-off messages, use the **attribute list** command in VRRS configuration mode. To configure VRRS to send only default attributes in VRRS accounting messages, use the **no** form of this command.

attribute list *list-name*

no attribute list

Syntax Description	<i>list-name</i>	Specifies a AAA accounting list, as defined by the aaa attribute list global configuration command.
---------------------------	------------------	--

Command Default	Default attributes are sent in VRRS accounting messages.
------------------------	--

Command Modes	VRRS configuration (config-vrrs)
----------------------	----------------------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines	Use the attribute list (VRRS) command to specify additional attributes to be included in both VRRS accounting-on and accounting-off messages. Before configuring this command, define a list name using the aaa attribute list global configuration command. If you enter a list name that is not defined in the aaa attribute list global configuration command, a warning message is displayed. However, this command is still accepted.
-------------------------	---

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, vrrs
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Type
- Attribute 44 Acct-Session-Id

Examples	The following example configures VRRS to use the AAA accounting list named vrrp-1-attr:
-----------------	---

```
Router(config)# aaa accounting vrrs default start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay "10"
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-name-1
```

```
Router(config-vrrs)# accounting delay 10  
Router(config-vrrs)# attribute list vrrp-1-attr
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
aaa attribute list	Defines a AAA attribute list locally on a router.
accounting delay (VRRS)	Specifies a delay time for sending accounting-off messages for VRRS.
accounting method (VRRS)	Enables VRRS accounting for a VRRP group.

bindid

To configure a bind ID, use the **bindid** command in SLB server farm configuration mode. To remove a bind ID from the server farm configuration, use the **no** form of this command.

bindid [*bind-id*]

no bindid [*bind-id*]

Syntax Description

bind-id (Optional) Bind ID number. The default bind ID is 0.

Defaults

The default bind ID is 0.

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.
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 one bind ID on each **bindid** command.

The bind ID allows a single physical server to be bound to multiple virtual servers, and to report a different weight for each one. Thus, the single real server is represented as multiple instances of itself, each having a different bind ID. Dynamic Feedback Protocol (DFP) uses the bind ID to identify for which instance of the real server a given weight is specified.

In general packet radio service (GPRS) load balancing, bind IDs are not supported. Therefore do not use the **bindid** command in a GPRS load-balancing environment.

Examples

The following example configures bind ID 309:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# bindid 309
```

Related Commands

Command	Description
ip slb dfp	Configures DFP, supplies an optional password, and enters DFP configuration mode.
show ip slb serverfarms	Displays information about the IOS SLB server farms.

calling-station-id

To configure an ASCII regular expression string to be matched against the calling station ID attribute for RADIUS load balancing, use the **calling-station-id** command in SLB RADIUS map configuration mode. To delete the calling station ID match string, use the **no** form of this command.

calling-station-id *string*

no calling-station-id *string*

Syntax Description

string

ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload.

For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the “Understanding Regular Expressions” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

None

Command Modes

SLB RADIUS map configuration (config-slb-radius-map)

Command History

Release

12.2(33)SRB

Modification

This command was introduced.

Usage Guidelines

For a given IOS SLB RADIUS map, you can configure a single **calling-station-id** command or a single **username (IOS SLB)** command, but not both.

Examples

The following example specifies that, for IOS SLB RADIUS map **1**, string **.919*** is to be matched against the calling station ID attribute in the RADIUS payload:

```
Router(config)# ip slb map 1 radius
Router(config-slb-radius-map)# calling-station-id .919*
```

Related Commands

Command	Description
ip slb map	Configures an IOS SLB protocol map and enters SLB map configuration mode.
show ip slb map	Displays information about IOS SLB protocol maps.
username	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

carrier-delay (tracking)

To enable Enhanced Object Tracking (EOT) to consider the carrier-delay timer when tracking the status of an interface, use the **carrier-delay** command in tracking configuration mode. To disable EOT from considering the carrier-delay timer when tracking the status of an interface, use the **no** form of this command.

carrier-delay

no carrier-delay

Command Default

EOT does not consider the carrier-delay timer configured on an interface when tracking the status of the interface.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If a link fails, by default there is a two-second timer that must expire before an interface and the associated routes are declared as being down. If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the switch is not aware that a link-down event occurred. You can configure the **carrier-delay seconds** command in interface configuration mode to extend the timer up to 60 seconds.

When Enhanced Object Tracking (EOT) is configured on an interface, the tracking may detect the interface is down before a configured carrier-delay timer has expired. This is because EOT looks at the interface state and does not consider the carrier delay timer. Use the **carrier-delay** command in tracking configuration mode to enable tracking to consider the carrier-delay timer configured on an interface.

Examples

The following example shows how to configure the tracking module to wait for the interface carrier-delay timer to expire before notifying clients of a state change:

```
Router(config)# track 101 interface ethernet1/0 line-protocol
Router(config-track)# carrier-delay
```

Related Commands

Command	Description
carrier-delay	Sets the carrier delay on an interface.
show track	Displays information about objects that are tracked by the tracking process.
track interface	Configures an interface to be tracked and to enter tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

Command	Description
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.
track resolution	Specifies resolution parameters for a tracked object.
track rtr	Tracks the state of a Cisco IOS SLAs operation and enters tracking configuration mode.
track timer	Specifies the interval in which the tracking process polls the tracked object.

clear fm slb counters

To clear Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters, use the **clear fm slb counters** command in privileged EXEC mode.

clear fm slb {inband | purge} counters

Syntax Description

inband	Clears FM IOS SLB inband counters.
purge	Clears FM IOS SLB purge counters.

Defaults

FM IOS SLB counters are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.

Examples

The following example clears the FM IOS SLB inband counters:

```
Router# clear fm slb inband counters
```

Related Commands

Command	Description
show fm slb counters	Displays information about the Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters.

clear ip accounting

To clear the active or checkpointed database when IP accounting is enabled, use the **clear ip accounting** command in privileged EXEC mode.

clear ip accounting [checkpoint]

Syntax Description

checkpoint	(Optional) Clears the checkpointed database.
-------------------	--

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **clear ip accounting** EXEC command clears the active database and creates the checkpointed database.

Examples

The following example clears the active database when IP accounting is enabled:

```
Router# clear ip accounting
```

Related Commands

Command	Description
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transit	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear ip icmp rate-limit

To clear all Internet Control Message Protocol (ICMP) unreachable rate-limiting statistics or all statistics for a specified interface, use the **clear ip icmp rate-limit** command in privileged EXEC mode.

clear ip icmp rate-limit [*interface-type interface-number*]

Syntax Description	<i>interface-type</i>	(Optional) Type of interface to be configured. Refer to the interface command in the <i>Cisco IOS Interface and Hardware Component Command Reference</i> , Release 12.4 for a list of valid interface types.
	<i>interface-number</i>	(Optional) Port, connector, or interface card number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the show interfaces command.

Defaults	All unreachable statistics for all devices are cleared.
-----------------	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.4(2)T	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples	The following example shows how to clear all unreachable statistics on all interfaces: Router# clear icmp rate-limit
-----------------	--

Related Commands	Command	Description
	ip icmp rate-limit unreachable	Limits the rate at which ICMP unreachable messages are generated for a destination.
	show ip icmp rate-limit	Displays all ICMP unreachable rate-limiting statistics or all statistics for a specified interface.

clear ip sctp statistics



Note

Effective with Cisco IOS Release 12.4(11)T, the **clear ip sctp statistics** command is replaced by the **clear sctp statistics** command. See the **clear sctp statistics** command for more information.

To clear statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **clear ip sctp statistics** command in privileged EXEC mode.

clear ip sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value. If this command is not entered, statistics counts for SCTP activity continue to be logged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.4(11)T	This command was replaced by the clear sctp statistics command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command clears both individual and overall statistics.

Examples

The following command shows how to empty the buffer that holds SCTP statistics. No output is generated from this command.

```
Router# clear ip sctp statistics
```

Related Commands

Command	Description
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays all currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

clear ip slb connections

To clear the IP IOS Server Load Balancing (IOS SLB) connections, use the **clear ip slb connections** command in privileged EXEC mode.

clear ip slb connections [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]

Syntax Description	firewallfarm <i>firewall-farm</i>	(Optional) Clears the IOS SLB connection database for the specified firewall farm.
	serverfarm <i>server-farm</i>	(Optional) Clears the IOS SLB connection database for the specified server farm.
	vserver <i>virtual-server</i>	(Optional) Clears the IOS SLB connection database for the specified virtual server.

Defaults The IOS SLB connection database is cleared for all firewall farms, server farms, and virtual servers.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.1(1)E	This command was introduced as part of the clear ip slb command.
	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(11b)E	This command was separated from the clear ip slb 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 In general packet radio service (GPRS) load balancing, the **clear ip slb connections** command clears connections, but does not clear sessions.

Examples The following example clears the connection database of server farm FARM1:

```
Router# clear ip slb connections serverfarm FARM1
```

The following example clears the connection database of virtual server VSERVER1:

```
Router# clear ip slb connections vserver VSERVER1
```

Related Commands

Command	Description
show ip slb conns	Displays information about active IOS SLB connections.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb serverfarms	Displays information about the IOS SLB server farms.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

clear ip slb counters

To clear the IP IOS Server Load Balancing (IOS SLB) counters, use the **clear ip slb counters** command in privileged EXEC mode.

clear ip slb counters [kal-ap]

Syntax Description	kal-ap	(Optional) clears only IP IOS SLB KeepAlive Application Protocol (KAL-AP) counters.
--------------------	---------------	---

Defaults	IP IOS SLB counters are not cleared.
----------	--------------------------------------

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.1(1)E	This command was introduced as part of the clear ip slb command.
	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(11b)E	This command was separated from the clear ip slb 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.
	12.2(33)SRC	The kal-ap keyword was added.

Examples	The following example clears the IP IOS SLB counters:
----------	---

```
Router# clear ip slb counters
```

Related Commands	Command	Description
	show ip slb stats	Displays IOS SLB statistics.

clear ip slb sessions

To clear the IP IOS Server Load Balancing (IOS SLB) sessions database, use the **clear ip slb sessions** command in privileged EXEC mode.

clear ip slb sessions [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]

Syntax Description	firewallfarm <i>firewall-farm</i>	(Optional) Clears the IOS SLB session database for the specified firewall farm.
	serverfarm <i>server-farm</i>	(Optional) Clears the IOS SLB session database for the specified server farm.
	vserver <i>virtual-server</i>	(Optional) Clears the IOS SLB session database for the specified virtual server.

Defaults	If no optional keywords or arguments are specified, the IOS SLB sessions database is cleared of all firewall farms, server farms, and virtual servers.
----------	--

Command Modes	Privileged EXEC (#)
---------------	---------------------

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 clears the session database of server farm FARM1:
----------	---

Router# **clear ip slb sessions serverfarm FARM1**

The following example clears the session database of virtual server VSERVER1:

Router# **clear ip slb sessions vserver VSERVER1**

Related Commands	Command	Description
	show ip slb firewallfarm	Displays information about the IOS SLB firewall farms.
	show ip slb sessions	Displays information about sessions handled by IOS SLB.
	show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

clear ip slb sticky asn msid

To clear an entry from an IOS Server Load Balancing (IOS SLB) Access Service Network (ASN) Mobile Station ID (MSID) sticky database, use the **clear ip slb sticky asn msid** command in privileged EXEC mode.

clear ip slb sticky asn msid *msid*

Syntax Description	<i>imsi</i> Clears the entry associated with the specified MSID from the IOS SLB ASN MSID sticky database.	
Defaults	None	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	12.2(33)SRE	This command was introduced.
Usage Guidelines	When you use this command to clear an entry from the IOS SLB ASN MSID sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the idle command in SLB virtual server configuration mode; the default timeout is 60 seconds.) To clear the session manually, use the clear ip slb sessions command in privileged EXEC mode.	
Examples	The following example clears the entry associated with MSID 001646013fc0 from the IOS SLB ASN MSID sticky database: Router# clear ip slb sticky asn msid 001646013fc0	
Related Commands	Command	Description
	show ip slb sticky	Displays information about the IOS Server Load Balancing (IOS SLB) sticky database.

clear ip slb sticky gtp imsi

To clear entries from an IOS Server Load Balancing (IOS SLB) general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database, use the **clear ip slb sticky gtp imsi** command in privileged EXEC mode.

clear ip slb sticky gtp imsi [*id imsi*]

Syntax Description	id imsi	Clears only the entry associated with the specified IMSI from the IOS SLB GTP IMSI sticky database.
---------------------------	----------------	---

Defaults	If you enter this command without the optional IMSI ID, all entries are cleared from the IOS SLB GTP IMSI sticky database.	
-----------------	--	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

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

Usage Guidelines	When you use this command to clear an entry from the IOS SLB GTP IMSI sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the idle command in SLB virtual server configuration mode; the default timeout is 30 seconds.) If the same user tries to create a new Packet Data Protocol (PDP) context before the session times out, using the same Network Service Access Point Identifier (NSAPI) but a different access point name (APN), IOS SLB forwards the request to the old server farm, even though the new APN should lead to a different server farm. To avoid this problem, clear the session manually by using the clear ip slb sessions command in privileged EXEC mode.
-------------------------	---

Examples	The following example clears all entries from the IOS SLB GTP IMSI sticky database:
-----------------	---

```
Router# clear ip slb sticky gtp imsi
```

Related Commands	Command	Description
	show ip slb sticky	Displays information about the IOS Server Load Balancing (IOS SLB) sticky database.

clear ip slb sticky radius

To clear entries from a IOS Server Load Balancing (IOS SLB) RADIUS sticky database, use the **clear ip slb sticky radius** command in privileged EXEC mode.

clear ip slb sticky radius { **calling-station-id** [*id string*] | **framed-ip** [*framed-ip* [*netmask*]] }

Syntax Description

calling-station-id	Clears entries from the IOS SLB RADIUS calling-station-ID sticky database.
id string	(Optional) Calling station ID of the entry to be cleared.
framed-ip	Clears entries from the IOS SLB RADIUS framed-IP sticky database.
framed-ip	(Optional) Framed-IP address of entries to be cleared.
netmask	(Optional) Subnet mask specifying a range of entries to be cleared.

Defaults

If no optional arguments are specified, all entries are cleared from the IOS SLB RADIUS calling-station-ID sticky database or framed-IP sticky database.

Command Modes

Privileged EXEC (#)

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(14)ZA5	The calling-station-id and id keywords and <i>string</i> argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you use this command to clear an entry from the IOS SLB RADIUS calling-station-ID sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the **idle** command in SLB virtual server configuration mode; the default timeout is 30 seconds.) If the same user tries to create a new Packet Data Protocol (PDP) context before the session times out, using the same Network Service Access Point Identifier (NSAPI) but a different access point name (APN), IOS SLB forwards the request to the old server farm, even though the new APN should lead to a different server farm. To avoid this problem, clear the session manually by using the **clear ip slb sessions** command in privileged EXEC mode.

Examples

The following example clears all entries from the IOS SLB RADIUS framed-IP sticky database:

```
Router# clear ip slb sticky radius framed-ip
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the IOS SLB sticky database.

clear ip tcp header-compression

To clear the TCP, UDP, and IP header-compression statistics, use the **clear ip tcp header-compression** command in privileged EXEC mode.

clear ip tcp header-compression *interface-type interface-number*

Syntax Description

<i>interface-number</i>	Specifies the interface type.
<i>interface-number</i>	Specifies the interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear the header-compression statistics for an ATM interface:

```
Router# clear ip tcp header-compression ATM2/0
```

Related Commands

Command	Description
show ip tcp header-compression	Displays statistics about TCP header compression.

clear ip traffic

To clear the global or system-wide IP traffic statistics for one or more interfaces, use the **clear ip traffic** command in privileged EXEC mode.

clear ip traffic [*interface type number*]

Syntax Description

interface *type number* (Optional) Clears the global or system-wide IP traffic statistics for a specific interface. If the **interface** keyword is used, the *type* and *number* arguments are required.

Command Default

Using the **clear ip traffic** command with no keywords or arguments clears the global or system-wide IP traffic statistics for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	This command was modified to include the optional interface keyword and associated <i>type</i> and <i>number</i> arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293: <i>Management Information Base for the Internet Protocol (IP)</i> .

Usage Guidelines

Using the **clear ip traffic** command with the optional **interface** keyword clears the ipIfStatsTable counters displayed for the specified interface and also clears the counters displayed by the **show ip traffic interface** command.

Examples

The following example clears the global or system-wide IP traffic statistics on all interfaces:

```
Router# clear ip traffic
```

Related Commands

Command	Description
show ip traffic	Displays the global or system-wide IP traffic statistics for one or more interfaces.

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear ip wccp** command in privileged EXEC mode.

clear ip wccp [**vrf** *vrf-name* {**web-cache** | *service-number*}] [**web-cache** | *service-number*]

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	(Optional) Directs the router to remove statistics for the web cache service.
<i>service-number</i>	(Optional) Number of the cache service to be removed. The number can be from 0 to 99.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CA	This command was introduced for Cisco 7200 and 7500 platforms.
11.2P	Support for this command was added to a variety of Cisco platforms.
12.0(3)T	This command was expanded to be explicit about service using the web-cache keyword and the <i>service-number</i> argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.
12.2(33)SRE	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics. If Cisco Cache Engines are used in your service group, the reverse proxy service is indicated by a value of 99.

Use the **clear ip wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

Use the **clear ip wccp vrf** *vrf-name* {**web-cache** | **service-number**} command to clear the WCCP counters for the specific WCCP service in the specified VRF.

Examples

The following example shows how to clear all statistics associated with the web cache service:

```
Router# clear ip wccp web-cache
```

Related Commands

Command	Description
clear platform software wccp	Clears WCCPv2 statistics on the Cisco ASR 1000 Series Routers.
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays global statistics related to the WCCP.

clear mls acl counters

To clear the multilayer switching (MLS) access control list (ACL) counters, use the **clear mls acl counters** command in privileged EXEC mode.

clear mls acl counters { **all** [**module num**] | **interface** *interface* *interface-number* [**loopback** *interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*] }

Syntax Description		
all		Clears all the MLS ACL counters for all interfaces.
module num		(Optional) Clears all the MLS ACL counters for the specified DFC.
interface <i>interface</i>		Clears counters that are associated with the specified interface; possible valid values are ethernet , fastethernet , gigabitethernet , and tengigabitethernet . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>		Module and port number; see the “Usage Guidelines” section for valid values.
loopback <i>interface-number</i>		(Optional) Specifies the loopback interface; valid values are from 0 to 2147483647.
null <i>interface-number</i>		(Optional) Specifies the null interface; the valid value is 0 .
port-channel <i>number</i>		(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan <i>vlan-id</i>		(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The valid values for *interface* include the **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on Cisco 7600 series routers that are configured with a WS-F6K-DFC3B-XL, release 2.1 and later.

If you enter the **clear mls acl counters all module** *num* command, all the MLS ACL counters for the specified DFC only are cleared. If you enter the **clear mls acl counters all** command without entering the **module** *num* keyword and argument, all the MLS ACL counters for only the non-DFC modules and the supervisor engines are cleared.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to reset the MLS ACL counters in all interfaces:

```
Router# clear mls acl counters all
```

Related Commands

Command	Description
show tcam interface	Displays information about the interface-based TCAM.

clear platform software wccp

To clear Web Cache Communication Protocol version 2 statistics on the Cisco ASR 1000 Series Routers, use the **clear platform software wccp** command in privileged EXEC mode.

clear platform software wccp {*slot* [**active** | **standby**] **statistics**} | {**counters** | **statistics**}

Syntax Description

<i>slot</i>	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: <ul style="list-style-type: none"> • F0—Embedded Service Processor slot 0 • F1—Embedded Service Processor slot 1 • FP—Embedded Service Processor • R0—Route Processor slot 0 • R1—Route Processor slot 1 • RP—Route Processor
active	Clears active instances.
standby	Clears standby instances.
statistics	Clears statistics counters.
counters	Clears packet processing counters.

Command Default

WCCPv2 statistics are not cleared.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear WCCPv2 statistics on Embedded-Service-Processor slot 0:

```
Router# clear platform software wccp F0 statistics
```

Related Commands

Command	Description
clear ip wccp	Removes WCCP statistics (counts) maintained on the router for a particular service.

clear sctp statistics

To clear statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **clear sctp statistics** command in privileged EXEC mode.

clear sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value. If this command is not entered, statistics counts for SCTP activity continue to be logged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the clear ip sctp statistics command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command clears both individual and overall statistics.


Examples

The following command shows how to empty the buffer that holds SCTP statistics. No output is generated from this command.

```
Router# clear sctp statistics
```

Related Commands

Command	Description
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays all currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.

 clear sctp statistics

Command	Description
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

clear sockets

To close all IP sockets and clear the underlying transport connections and data structures, use the **clear sockets** command in privileged EXEC mode.

clear sockets *process-id*

Syntax Description

<i>process-id</i>	Identifier of the IP process to be cleared.
-------------------	---

Command Default

IP socket information is not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Using this command results in an abortive close for TCP connections and Stream Control Transfer Protocol (SCTP) associations. When this command is entered, TCP connections abort by sending an RST (reset) and SCTP associations abort by sending an ABORT signal to the peer.

Use the **show processes** command to display the list of running processes and their associated process IDs.

You can use the **show sockets detail** command to confirm all open sockets have been cleared.

Examples

The following example shows how to close all sockets for IP process 35:

```
Router# clear sockets 35
```

```
All sockets (TCP, UDP and SCTP) for this process will be cleared.  
Do you want to proceed? [yes/no]: y  
Cleared sockets for PID 35
```

Related Commands

Command	Description
show processes	Displays information about the active processes.
show sockets	Displays IP socket information.
show udp	Displays IP socket information about UDP processes.

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in privileged EXEC command.

clear tcp statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

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

Examples The following example clears all TCP statistics:

```
Router# clear tcp statistics
```

Related Commands	Command	Description
	show tcp statistics	Displays TCP statistics.

clear time-range ipc

To clear the time-range interprocess communications (IPC) message statistics and counters between the Route Processor and the line card, use the **clear time-range ipc** command in privileged EXEC mode.

clear time-range ipc

Syntax Description	This command has no argument or keywords.
---------------------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples	The following example clears the time-range IPC statistics and counters:
-----------------	--

```
Router# clear time-range ipc
```

Related Commands	Command	Description
	debug time-range ipc	Enables debugging output for monitoring the time-range IPC messages between the Route Processor and the line card.
	show time-range ipc	Displays the statistics about the time-range IPC messages between the Route Processor and line card.

client (virtual server)

To define which clients are allowed to use the virtual server, use the **client** command in Server Load Balancing (SLB) virtual server configuration mode. To remove a client definition from the SLB configuration, use the **no** form of this command.

client {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}

no client {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}

Syntax Description

<i>ipv4-address</i>	Client IPv4 address. The default is 0.0.0.0 (all clients).
<i>netmask</i>	Client IPv4 network mask. The default is 0.0.0.0 (all subnets).
exclude	(Optional) Ignores connections initiated by the client IPv4 address from the load-balancing scheme.
gtp carrier-code	For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the virtual server to accept Packet Data Protocol (PDP) context creates only from the specified International Mobile Subscriber Identity (IMSI) carrier code.
<i>code</i>	(Optional) For GTP cause code inspection, identifies the IMSI carrier code from which this virtual server is to accept PDP context creates. The code has the format: <p style="text-align: center;">mcc <i>mcc-code</i> mnc <i>mnc-code</i></p> <p>where:</p> <ul style="list-style-type: none"> <i>mcc-code</i> is the Mobile Country Code (MCC) <i>mnc-code</i> is the Mobile Network Code (MNC) <p>If you do not specify a <i>code</i>, the virtual server accepts PDP context creates from any IMSI carrier code.</p>

Command Default

The default client IPv4 address is 0.0.0.0 (all clients).
The default client IPv4 network mask is 0.0.0.0 (all subnets).
Taken together, the default is client 0.0.0.0 0.0.0.0 (allows all clients on all subnets to use the virtual server).
If you specify **gtp carrier-code** and you do not specify a *code*, the virtual server accepts PDP context creates from any IMSI carrier code.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(1)E	The exclude keyword was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The gtp carrier-code keyword and <i>code</i> argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can use more than one client command to define more than one client.

The *netmask* value is applied to the source IPv4 address of incoming connections. The result must match the *ipv4-address* value for the client to be allowed to use the virtual server.

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 IPv4 address from the load-balancing scheme.
- Configure IPv4 addresses on the IOS SLB device that are Layer 3-adjacent to the real servers used by the virtual server.

Configure separate **client** commands to specify the clients that can use the virtual server, and to specify the IMSI carrier code from which the virtual server is to accept PDP context creates.

Dual-stack support for GTP load balancing does not support this command.

Examples

The following example allows clients from only 10.4.4.0 access to the virtual server:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# client 10.4.4.0 255.255.255.0
```

Related Commands

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

credentials (HTTP probe)

To configure basic authentication values for the HTTP IOS Server Load Balancing (IOS SLB) probe, use the **credentials** command in HTTP probe configuration mode. To remove a **credentials** configuration, use the **no** form of this command.

credentials *username* [*password*]

no credentials *username* [*password*]

Syntax Description

<i>username</i>	Authentication username of the HTTP probe header. The character string is limited to 15 characters.
<i>password</i>	(Optional) Authentication password of the HTTP probe header. The character string is limited to 15 characters.

Defaults

Basic authentication values for the HTTP IOS SLB probe are not configured.

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.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, sets the HTTP authentication to username Username1, and sets the password to develop:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# credentials Username1 develop
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.