

idle (firewall farm datagram protocol)

To specify the minimum time IOS Server Load Balancing (IOS SLB) maintains connection information in the absence of packet activity, use the **idle** command in firewall farm datagram protocol configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description	<i>duration</i>	Idle connection timer duration in seconds. Valid values range from 10 to 65535 seconds. The default is 3600 seconds (1 hour).
---------------------------	-----------------	---

Defaults The default idle duration is 3600 seconds.

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 instructs IOS SLB to maintain connection information for an idle connection for 120 seconds:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
Router(config-slb-fw-udp)# idle 120
```

Related Commands	Command	Description
	protocol datagram	Enters firewall farm datagram protocol configuration mode.
	show ip slb firewallfarm	Displays information about the firewall farm configuration.

idle (firewall farm TCP protocol)

To specify the minimum time IOS Server Load Balancing (IOS SLB) maintains connection information in the absence of packet activity, use the **idle** command in firewall farm TCP protocol configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description	<i>duration</i>	Idle connection timer duration in seconds. Valid values range from 10 to 65535 seconds. The default is 3600 seconds (1 hour).
---------------------------	-----------------	---

Defaults	The default idle duration is 3600 seconds.
-----------------	--

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

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

Usage Guidelines	<p>TCP connections that do not send flows or keepalives before the idle timer expires are assumed to be inactive and are reset (RST).</p> <p>If you are configuring an idle timer for HTTP flows, choose a low number such as 120 seconds as a starting point. A low number ensures that the IOS SLB connection database maintains a manageable size if problems at the server, client, or network result in a large number of connections. However, do not choose a value under 60 seconds; such a low value can reduce the efficiency of IOS SLB.</p>
-------------------------	---

Examples	The following example instructs IOS SLB to maintain connection information for an idle connection for 120 seconds:
-----------------	--

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# idle 120
```

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

idle (virtual server)

To specify the minimum time the IOS Server Load Balancing (IOS SLB) maintains connection information in the absence of packet activity, use the **idle** command in SLB virtual server configuration mode. To restore the default idle duration value, use the **no** form of this command.

```
idle [asn r6 request duration | gtp imsi duration [query [max-queries]] | gtp request duration | ipmobile request duration | radius {request | framed-ip} duration]
```

```
no idle [asn r6 request duration | gtp imsi duration [query [max-queries]] | gtp request duration | ipmobile request duration | radius {request | framed-ip} duration]
```

Syntax Description	
asn r6 request	(Optional) For load balancing across a set of Access Service Network (ASN) gateways, configures the duration for which IOS SLB keeps the session object. If a Mobile Station (MS) Pre-Attachment Ack is received before the timer expires, IOS SLB resets the timer.
<i>duration</i>	Idle connection timer duration in seconds. Valid values range from 4 to 65535 seconds. For GTP IMSI, you can specify 0 to disable the timer and prevent GTP IMSI sticky database objects from timing out. The default values are: <ul style="list-style-type: none"> • 60 seconds in ASN R6 load balancing. • 0 seconds for objects in the GTP IMSI sticky database. • 10 seconds in the Home Agent Director. • 30 seconds in GPRS load balancing. • 30 seconds for RADIUS entries in the IOS SLB session database. • 7200 seconds for entries in the IOS SLB RADIUS framed-IP sticky database. • 3600 seconds (1 hour) in all other environments.
gtp imsi	(Optional) For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the duration for objects in the GTP International Mobile Subscriber ID (IMSI) sticky database.
query	(Optional) Query the Cisco gateway GPRS support node (GGSN) before deleting any GTP IMSI sticky objects. The default is not to query the GGSN.
<i>max-queries</i>	(Optional) Maximum number of queries to send when there is no response from the GGSN. Valid range is 1 to 10 queries. The default value is 5 queries.
gtp request	(Optional) For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the duration for Packet Data Protocol (PDP) context create, update, or delete request messages to a real gateway GPRS support node (GGSN) to go unanswered, before IOS SLB cleans up the session object.

ipmobile request	(Optional) For Home Agent Director, configures the duration for IOS SLB to wait for a Mobile IP Registration Request (RRQ), before IOS SLB cleans up the session object.
radius request	(Optional) Configures the duration for RADIUS entries in the IOS SLB session database.
radius framed-ip	(Optional) Configures the duration for entries in the IOS SLB RADIUS framed-IP sticky database.

Defaults

The default idle duration is:

- 60 seconds in ASN R6 load balancing.
- 0 seconds for objects in the GTP IMSI sticky database.
- 10 seconds in the Home Agent Director
- 30 seconds in GPRS load balancing
- 30 seconds for RADIUS entries in the IOS SLB session database
- 7200 seconds for entries in the IOS SLB RADIUS framed-IP sticky database
- 3600 seconds (1 hour) in all other environments

The default setting for the **query** keyword is no queries.

The default setting for the *max-queries* argument is 5 queries.

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(9)E	This command was modified to support GPRS load balancing.
12.1(11b)E	This command was modified to support RADIUS load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The gtp request keywords were added.
12.2(14)ZA2	The ipmobile request keywords were added.
12.2(18)SXE	The gtp imsi keywords were added.
12.2(18)SXF	The query keyword and <i>max-queries</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC1	The asn r6 request keywords were added.

Usage Guidelines

TCP connections that do not send flows or keepalives before the idle timer expires are assumed to be inactive and are reset (RST).

If you are configuring an idle timer for HTTP flows, choose a low number such as 120 seconds as a starting point. A low number ensures that the IOS SLB connection database maintains a manageable size if problems at the server, client, or network result in a large number of connections. However, do not choose a value under 60 seconds (except in GPRS load balancing); such a low value can reduce the efficiency of the IOS SLB feature.

In most environments, the idle timer times out data paths. However, in GPRS load balancing, it times out the session context for signaling paths (not data paths).

In GPRS load balancing without GTP cause code inspection enabled, you must specify an idle timer greater than the longest possible interval between PDP context requests on the serving GPRS support node (SGSN). The longest interval can be expressed using the following algorithm:

$$\text{Longest interval} = T3 \times 2^{(N3-2)}$$

where T3 is the SGSN's T3-RESPONSE counter value and N3 is the SGSN's N3-REQUESTS counter value.

For example, if the T3-RESPONSE counter value is 3 and the N3-REQUESTS counter value is 6, then:

$$\text{Longest interval} = 3 \times 2^{(6-2)} = 3 \times 2^4 = 3 \times 16 = 48 \text{ seconds}$$

Given those values, you must specify an idle timer of at least 49 seconds.

Examples

The following example instructs IOS SLB to maintain connection information for an idle connection for 120 seconds:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# idle 120
```

Related Commands

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

inservice (DFP agent)

To enable the Dynamic Feedback Protocol (DFP) agent for communication with a DFP manager, use the **inservice** command in DFP agent configuration mode. To remove the DFP agent from service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The DFP agent is inactive.

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

A DFP agent is inactive until both of the following conditions are met:

- The DFP agent has been enabled using the **inservice (DFP agent)** command.
- The client subsystem has changed the DFP agent's state to **ACTIVE**.

When you use the **no** form of this command to remove a DFP agent from service, the DFP agent closes all open connections, and no new connections are assigned.

Examples

In the following example, the DFP agent is enabled for communication with a DFP manager:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# inservice
```

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.

Command	Description
ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.

inservice (firewall farm)

To enable the firewall farm for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in firewall farm configuration mode. To remove the firewall farm from service, use the **no** form of this command.

inservice [*standby group-name*]

no inservice [*standby group-name*]

Syntax Description

standby	(Optional) Configures the Hot Standby Router Protocol (HSRP) standby firewall farm for use with stateless and stateful backup.
<i>group-name</i>	(Optional) HSRP group name with which the IOS SLB firewall farm is associated.

Defaults

The firewall farm is defined to IOS SLB but is not used.

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

When you use the **no** form of this command to remove a firewall farm from service, the firewall farm acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

Examples

In the following example, the firewall farm is enabled for use by the IOS SLB feature:

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

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

inservice (firewall farm real server)

To enable the firewall for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in firewall farm real server configuration mode. To remove the firewall from service, use the **no** form of this command.

inservice

no inservice

Syntax Description This command has no arguments or keywords.

Defaults The firewall is defined to IOS SLB but is not used.

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

IOS SLB firewall load balancing uses probes to detect failures. Therefore, if you have not configured a probe, the firewall is not placed in service.

When you use the **no** form of this command to remove a firewall from service, the firewall acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

Examples

In the following example, the firewall is enabled for use by the IOS SLB feature:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# real 10.10.1.1
Router(config-slb-fw-real)# inservice
```

Related Commands

Command	Description
real (firewall farm)	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

inservice (server farm real server)

To enable the real server for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in SLB server farm real server configuration mode. To remove the real server from service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The real server is defined to IOS SLB but is not used.

Command Modes

SLB server farm real server configuration (config-slb-sfarm-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

In the following example, the real server is enabled for use by the IOS SLB feature:

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

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.

inservice (server farm virtual server)

To enable the virtual server for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in SLB server farm virtual server configuration mode. To remove the virtual server from service, use the **no** form of this command.

inservice [**standby** *group-name*] [**active**]

no inservice [**standby** *group-name*]

Syntax Description

standby	(Optional) Configures the Hot Standby Router Protocol (HSRP) standby virtual server for use with stateless and stateful backup.
<i>group-name</i>	(Optional) HSRP group name with which the IOS SLB virtual server is associated.
active	(Optional) Enables the virtual server to stop answering Internet Control Message Protocol (ICMP) requests if all real servers associated with the virtual server are inactive.

Defaults

The virtual server is defined to IOS SLB but is not used.

Command Modes

SLB server farm virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(1)E	The standby keyword and <i>group-name</i> argument were 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.
12.2(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 active keyword was added.

Usage Guidelines

When you use the **no** form of this command to remove a virtual server from service, the virtual server acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

If the **active** keyword is configured, and all of the real servers that are associated with the virtual server are inactive, the following actions occur:

- The virtual server is placed in the INOP_REAL state.
- An SNMP trap is generated for the virtual server's state transition.
- The virtual server stops answering ICMP requests.

Examples

In the following example, the virtual server is enabled for use by the IOS SLB feature:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# inservice
```

Related Commands

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

interval (custom UDP probe)

To configure a custom User Datagram Protocol (UDP) probe interval, use the **interval** command in custom UDP probe configuration mode. To remove a custom UDP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.
----------------	--

Defaults

The default custom UDP probe interval value is 10 seconds.

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 configuration mode, and configures the custom UDP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# interval 11
```

Related Commands

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

interval (DFP agent)

To configure a Dynamic Feedback Protocol (DFP) agent weight recalculation interval, use the **interval** command in DFP agent configuration mode. To restore the default setting, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds to wait before recalculating weights for the DFP manager. The valid range is from 5 to 65535 seconds. The default is 10 seconds.
---------------------------	----------------	--

Defaults	The default interval value is 10 seconds.
-----------------	--

Command Modes	DFP agent configuration (config- <i>dfp</i>)
----------------------	---

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 DFP agent sends a new weight to the DFP manager only if the new weight is different from the old weight. If the new weight is the same as the old weight, it is not sent to the DFP manager.
-------------------------	--

Examples	The following example shows how to configure the DFP agent to recalculate weights every 11 seconds: <pre>Router(config)# ip dfp agent slb Router(config-dfp)# interval 11</pre>
-----------------	--

Related Commands	Command	Description
	agent	Identifies a DFP agent to which IOS SLB can connect.
	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.

interval (DNS probe)

To configure a DNS probe interval, use the **interval** command in DNS probe configuration mode. To remove a DNS probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.
---------------------------	----------------	--

Defaults The default DNS probe interval value is 10 seconds.

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 configuration mode, and configures the DNS probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# interval 11
```

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.

interval (HTTP probe)

To configure an HTTP probe interval, use the **interval** command in HTTP probe configuration mode. To remove an HTTP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 8 seconds.
--------------------	----------------	---

Defaults The default HTTP probe interval value is 8 seconds.

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 configuration mode, and configures the HTTP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# interval 11
```

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.

interval (ping probe)

To configure a ping probe interval, use the **interval** command in ping probe configuration mode. To remove a ping probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 1 second.
---------------------------	----------------	--

Defaults The default ping probe interval value is 1 second.

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

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

Examples The following example configures a ping probe named PROBE1, enters ping configuration mode, and configures the ping probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# interval 11
```

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.

interval (TCP probe)

To configure a TCP probe interval, use the **interval** command in TCP probe configuration mode. To remove a TCP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.
---------------------------	----------------	--

Defaults The default TCP probe interval value is 10 seconds.

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 configuration mode, and configures the TCP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# interval 11
```

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.

interval (WSP probe)

To configure a Wireless Session Protocol (WSP) probe interval, use the **interval** command in WSP probe configuration mode. To remove a WSP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

<i>seconds</i>	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 8 seconds.
----------------	---

Defaults

The default WSP probe interval value is 8 seconds.

Command Modes

WSP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(5a)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 ping probe named PROBE3, enters WSP probe configuration mode, and configures the WSP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE3 wsp
Router(config-slb-probe)# interval 11
```

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.

ip accounting

To enable IP accounting on an interface, use the **ip accounting** command in interface configuration mode. To disable IP accounting, use the **no** form of this command.

ip accounting [**access-violations**] [**output-packets**]

no ip accounting [**access-violations**] [**output-packets**]

Syntax Description		
	access-violations	(Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.
	output-packets	(Optional) Enables IP accounting based on the IP packets output on the interface.

Defaults Disabled

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The access-violations keyword was added.
	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 **ip accounting** command records the number of bytes (IP header and data) and packets switched through the system on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the router access server or terminating in this device is not included in the accounting statistics.

If you specify the **access-violations** keyword, the **ip accounting** command provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data might also indicate that you should verify IP access list configurations.

To receive a logging message on the console when an extended access list entry denies a packet access (to log violations), you must include the **log** keyword in the **access-list** (IP extended) or **access-list** (IP standard) command.

Statistics are accurate even if IP fast switching or IP access lists are being used on the interface. If the **access-violations** keyword is specified and any IP access list is being used on an interface, then only process switching can generate accurate statistics (IP fast switching or CEF cannot).

IP accounting disables autonomous switching, SSE switching, and distributed switching (dCEF) on the interface. IP accounting will cause packets to be switched on the Route Switch Processor (RSP) instead of the Versatile Interface Processor (VIP), which can cause performance degradation.

Examples

The following example enables IP accounting on Ethernet interface 0:

```
interface ethernet 0
 ip accounting
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
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-transits	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.

ip accounting-list

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** command in global configuration mode. To remove a filter definition, use the **no** form of this command.

ip accounting-list *ip-address wildcard*

no ip accounting-list *ip-address wildcard*

Syntax Description

<i>ip-address</i>	IP address in dotted decimal format.
<i>wildcard</i>	Wildcard bits to be applied to the <i>ip-address</i> argument.

Defaults

No filters are defined.

Command Modes

Global configuration (config)

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 *wildcard* argument is a 32-bit quantity written in dotted-decimal format. Address bits corresponding to wildcard bits set to 1 are ignored in comparisons; address bits corresponding to wildcard bits set to zero are used in comparisons.

Examples

The following example adds all hosts with IP addresses beginning with 192.31 to the list of hosts for which accounting information will be kept:

```
ip accounting-list 192.31.0.0 0.0.255.255
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.

Command	Description
ip accounting-transits	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.

ip accounting mac-address

To enable IP accounting on a LAN interface based on the source and destination Media Access Control (MAC) address, use the **ip accounting mac-address** command in interface configuration mode. To disable IP accounting based on the source and destination MAC address, use the **no** form of this command.

ip accounting mac-address {input | output}

no ip accounting mac-address {input | output}

Syntax Description	input	output
	Performs accounting based on the source MAC address on received packets.	Performs accounting based on the destination MAC address on transmitted packets.

Defaults Disabled

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	11.1CC	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.
	12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines This feature is supported on Ethernet, Fast Ethernet, and FDDI interfaces.

To display the MAC accounting information, use the **show interface mac EXEC** command.

MAC address accounting provides accounting information for IP traffic based on the source and destination MAC address on LAN interfaces. This calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent. With MAC address accounting, you can determine how much traffic is being sent to and/or received from various peers at NAPS/peering points.

Examples The following example enables IP accounting based on the source and destination MAC address for received and transmitted packets:

```
interface ethernet 4/0/0
 ip accounting mac-address input
 ip accounting mac-address output
```

Cisco uBR10012 Universal Broadband Router

The following example enables IP accounting based on the source MAC address for received packets on a Gigabit Ethernet interface:

```
Router#configure terminal  
Router(config)#interface GigabitEthernet3/0/0  
Router(config-if)#ip accounting mac-address input
```

Related Commands

Command	Description
show interface mac	Displays MAC accounting information for interfaces configured for MAC accounting.

ip accounting precedence

To enable IP accounting on any interface based on IP precedence, use the **ip accounting precedence** command in interface configuration mode. To disable IP accounting based on IP precedence, use the **no** form of this command.

ip accounting precedence {input | output}

no ip accounting precedence {input | output}

Syntax Description

input	Performs accounting based on IP precedence on received packets.
output	Performs accounting based on IP precedence on transmitted packets.

Command Default

IP accounting is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

To display IP precedence accounting information, use the **show interface precedence EXEC** command.

The precedence accounting feature provides accounting information for IP traffic, summarized by IP precedence values. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on IP precedence. This feature is supported on all interfaces and subinterfaces and supports Cisco Express Forwarding (CEF), dCEF, flow, and optimum switching.

Examples

The following example enables IP accounting based on IP precedence for received and transmitted packets:

```
interface ethernet 4/0/0
 ip accounting precedence input
 ip accounting precedence output
```

Related Commands

Command	Description
show interface precedence	Displays precedence accounting information for an interface configured for precedence accounting.

ip accounting-threshold

To set the maximum number of accounting entries to be created, use the **ip accounting-threshold** command in global configuration mode. To restore the default number of entries, use the **no** form of this command.

ip accounting-threshold *threshold*

no ip accounting-threshold *threshold*

Syntax Description	<i>threshold</i>	Maximum number of entries (source and destination address pairs) that the Cisco IOS software accumulates.
---------------------------	------------------	---

Defaults The default maximum number of accounting entries is 512 entries.

Command Modes Global configuration (config)

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 accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates, preventing IP accounting from possibly consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. Overflows will be recorded; see the monitoring commands for display formats.

The default accounting threshold of 512 entries results in a maximum table size of 12,928 bytes. Active and checkpointed tables can reach this size independently.

Examples The following example sets the IP accounting threshold to 500 entries:

```
ip accounting-threshold 500
```

Related Commands	Command	Description
	clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
	ip accounting	Enables IP accounting on an interface.
	ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.

Command	Description
ip accounting-transits	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.

ip accounting-transits

To control the number of transit records that are stored in the IP accounting database, use the **ip accounting-transits** command in global configuration mode. To return to the default number of records, use the **no** form of this command.

ip accounting-transits *count*

no ip accounting-transits

Syntax Description

<i>count</i>	Number of transit records to store in the IP accounting database.
--------------	---

Defaults

The default number of transit records that are stored in the IP accounting database is 0.

Command Modes

Global configuration (config)

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

Transit entries are those that do not match any of the filters specified by **ip accounting-list** global configuration commands. If no filters are defined, no transit entries are possible.

To maintain accurate accounting totals, the Cisco IOS software maintains two accounting databases: an active and a checkpointed database.

Examples

The following example specifies that no more than 100 transit records are stored:

```
ip accounting-transits 100
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
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.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restore the default IP broadcast address, use the **no** form of this command.

ip broadcast-address [*ip-address*]

no ip broadcast-address [*ip-address*]

Syntax Description	<i>ip-address</i> (Optional) IP broadcast address for a network.
---------------------------	--

Defaults	Default address: 255.255.255.255 (all ones)
-----------------	---

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

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.

Examples	The following example specifies an IP broadcast address of 0.0.0.0:
-----------------	---

```
ip broadcast-address 0.0.0.0
```

ip casa

To configure the router to function as a forwarding agent, use the **ip casa** command in global configuration mode. To disable the forwarding agent, use the **no** form of this command.

```
ip casa control-address igmp-address [udp-limit]
```

```
no ip casa
```

Syntax Description	control-address	IP address of the forwarding agent side of the services manager and forwarding agent tunnel used for sending signals. This address is unique for each forwarding agent.
	igmp-address	Interior Gateway Management Protocol (IGMP) address on which the forwarding agent will listen for wildcard and fixed affinities.
	udp-limit	(Optional) Maximum User Datagram Protocol (UDP) queue length; valid values are from 50 to 65535. The default is 256.

Defaults No default behavior or values.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2(17d)SXB1	Support for this command was added for Catalyst 6500 series switches.
	12.2(18)SXF6	The <i>udp-limit</i> argument was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines If more than the maximum *udp-limit* value arrives in a burst, the Cisco Appliance Services Architecture (CASA) wildcard updates from the service manager might get dropped.
The *control-address* value is unique for each forwarding agent.

Examples The following example specifies the Internet address (10.10.4.1) and IGMP address (224.0.1.2) for the forwarding agent and sets the UDP queue length to 300:

```
ip casa 10.10.4.1 224.0.1.2 300
```

Related Commands	Command	Description
	forwarding-agent	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.

ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) sets up or tears down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip cef traffic-statistics [*load-interval seconds*] [*update-rate seconds*]

no ip cef traffic-statistics

Syntax Description

load-interval <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> intervals are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the ip nhrp trigger-svc command.) The load-interval range is from 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate <i>seconds</i>	(Optional) Frequency that the port adapter sends the accounting statistics to the Route Processor (RP). When using NHRP in distributed Cisco Express Forwarding switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Defaults

Load interval: 30 seconds
Update rate: 10 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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 **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the Cisco Express Forwarding traffic load statistics. The thresholds in the **ip nhrp trigger-svc** command are measured during a sampling interval of 30 seconds, by default. To change that interval over which that threshold is determined, use the **load-interval** *seconds* option of the **ip cef traffic-statistics** command.

When NHRP is configured on a Cisco Express Forwarding switching node with a Versatile Interface Processor (VIP2) adapter, you must make sure the **update-rate** keyword is set to 5 seconds.

Other Cisco IOS features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip dfp agent

To identify a Dynamic Feedback Protocol (DFP) agent subsystem and enter DFP agent configuration mode, use the **ip dfp agent** command in global configuration mode. To remove the DFP agent identification, use the **no** form of this command.

ip dfp agent *subsystem-name*

no ip dfp agent *subsystem-name*

Syntax Description

<i>subsystem-name</i>	Character string used to identify the DFP agent subsystem: <ul style="list-style-type: none"> • slb for IOS SLB • mobileip for Mobile IP and the Home Agent Director <p>The subsystem name enables the subsystem to send weights to a DFP manager. The subsystem name is limited to 15 characters.</p>
-----------------------	--

Defaults

No DFP agent subsystem is defined.

Command Modes

Global configuration (config)

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	The mobileip subsystem name was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To discover the subsystem names that are available in your network, enter the **ip dfp agent ?** command.

Examples

The following example identifies a DFP agent subsystem named **slb**:

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

Related Commands

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

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast [*access-list-number* | *extended access-list-number*]

no ip directed-broadcast [*access-list-number* | *extended access-list-number*]

Syntax Description

<i>access-list-number</i>	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.
<i>extended access-list-number</i>	(Optional) Extended access list number in the range from 1300 to 2699.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The default behavior changed to directed broadcasts being dropped.
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

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is “exploded” as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If **directed broadcast** is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

**Note**

Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

Examples

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ip directed-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip forward-protocol

To specify which protocols and ports the router forwards when forwarding broadcast packets, use the **ip forward-protocol** command in global configuration mode. To remove a protocol or port, use the **no** form of this command.

```
ip forward-protocol { udp [port] | nd | sdns }
```

```
no ip forward-protocol { udp [port] | nd | sdns }
```

Syntax Description

udp	Forwards User Datagram Protocol (UDP) packets. See the “Usage Guidelines” section for a list of port numbers forwarded by default.
<i>port</i>	(Optional) Destination port that controls which UDP services are forwarded.
nd	Forwards Network Disk (ND) packets. This protocol is used by older diskless Sun workstations.
sdns	Secure Data Network Service.

Defaults

Enabled

Command Modes

Global configuration (config)

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

Enabling a helper address or UDP flooding on an interface causes the Cisco IOS software to forward particular broadcast packets. You can use the **ip forward-protocol** command to specify exactly which types of broadcast packets you would like to have forwarded. A number of commonly forwarded applications are enabled by default. Enabling forwarding for some ports [for example, Routing Information Protocol (RIP)] may be hazardous to your network.

If you use the **ip forward-protocol** command, specifying only UDP without the port enables forwarding and flooding on the default ports.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP). DHCP is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the software. The DHCP server now receives broadcasts from the DHCP clients.

If an IP helper address is defined, UDP forwarding is enabled on default ports. If UDP flooding is configured, UDP flooding is enabled on the default ports.

If a helper address is specified and UDP forwarding is enabled, broadcast packets destined to the following port numbers are forwarded by default:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- Boot Protocol (BOOTP) client and server packets (ports 67 and 68)
- TACACS service (port 49)
- IEN-116 Name Service (port 42)

**Note**

If UDP port 68 is used as the destination port number, it is not forwarded by default.

Examples

The following example defines a helper address and uses the **ip forward-protocol** command. Using the **udp** keyword without specifying any port numbers will allow forwarding of UDP packets on the default ports.

```
ip forward-protocol udp
interface ethernet 1
 ip helper-address 10.24.42.2
```

ip forward-protocol spanning-tree

To permit IP broadcasts to be flooded throughout the internetwork in a controlled fashion, use the **ip forward-protocol spanning-tree** command in global configuration mode. To disable the flooding of IP broadcasts, use the **no** form of this command.

ip forward-protocol spanning-tree [**any-local-broadcast**]

no ip forward-protocol spanning-tree [**any-local-broadcast**]

Syntax Description

any-local-broadcast (Optional) Accept any local broadcast when flooding.

Defaults

Disabled

Command Modes

Global configuration (config)

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

A packet must meet the following criteria to be considered for flooding:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; major-net broadcast for the receiving interface if the **no ip classless** command is also configured; or any local IP broadcast address if the **ip forward-protocol spanning-tree any-local-broadcast** command is configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be User Datagram Protocol (UDP) (17).
- The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, ND, or BOOTP packet, or a UDP port specified by the **ip forward-protocol udp** command.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** command on the output interface. The destination address can be set to any desired address. Thus, the destination address may change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

After a decision has been made to send the datagram out on an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is therefore subject to access lists, if they are present on the output interface.

The **ip forward-protocol spanning-tree** command uses the database created by the bridging Spanning-Tree Protocol. Therefore, the transparent bridging option must be in the routing software, and bridging must be configured on each interface that is to participate in the flooding in order to support this capability.

If an interface does not have bridging configured, it still will be able to receive broadcasts, but it will never forward broadcasts received on that interface. Also, it will never use that interface to send broadcasts received on a different interface.

If no actual bridging is desired, you can configure a type-code bridging filter that will deny all packet types from being bridged. Refer to the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more information about using access lists to filter bridged traffic. The spanning-tree database is still available to the IP forwarding code to use for the flooding.

The spanning-tree-based flooding mechanism forwards packets whose contents are all ones (255.255.255.255), all zeros (0.0.0.0), and, if subnetting is enabled, all networks (10.108.255.255 as an example in the network number 10.108.0.0). This mechanism also forward packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 10.108.0.0).

This command is an extension of the **ip helper-address** command, in that the same packets that may be subject to the helper address and forwarded to a single network can now be flooded. Only one copy of the packet will be put on each network segment.

Examples

The following example permits IP broadcasts to be flooded through the internetwork in a controlled fashion:

```
ip forward-protocol spanning-tree
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
ip forward-protocol turbo-flood	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip forward-protocol turbo-flood

To speed up flooding of User Datagram Protocol (UDP) datagrams using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip forward-protocol turbo-flood [udp-checksum]

no ip forward-protocol turbo-flood [udp-checksum]

Syntax Description	udp-checksum (Optional) UDP checksum.								
Command Default	Disabled								
Command Modes	Global configuration (config)								
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> <tr> <td>12.2(17d)SXB7</td> <td>Support for this command was introduced on the Supervisor Engine 720.</td> </tr> <tr> <td>12.2(33)SRA</td> <td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.	12.2(17d)SXB7	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.
Release	Modification								
10.0	This command was introduced.								
12.2(17d)SXB7	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 Used in conjunction with the **ip forward-protocol spanning-tree** command, this command is supported over Advanced Research Projects Agency (ARPA)-encapsulated Ethernets, FDDI, and High-Level Data Link Control (HDLC) encapsulated serials, but is not supported on Token Rings. As long as the Token Rings and the non-HDLC serials are not part of the bridge group being used for UDP flooding, turbo flooding will behave normally.

When you enter the **ip forward-protocol turbo-flood** command, the outgoing UDP packets have a NULL checksum. If you want to have UDP checksums on all outgoing packets, you must enter the **ip forward-protocol turbo-flood udp-checksum** command.

Examples The following is an example of a two-port router using this command:

```
ip forward-protocol turbo-flood
ip forward-protocol spanning-tree
!
interface ethernet 0
 ip address 10.9.1.1
 bridge-group 1
!
interface ethernet 1
 ip address 10.9.1.2
 bridge-group 1
!
bridge 1 protocol dec
```

The following example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm and include the UDP checksums on all outgoing packets:

```
ip forward-protocol turbo-flood udp-checksum
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports are forwarded by the router when forwarding broadcast packets.
ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

ip helper-address

To enable the forwarding of User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ip helper-address** command in interface configuration mode. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

```
ip helper-address [vrf name | global] address [redundancy vrg-name]
```

```
no ip helper-address [vrf name | global] address [redundancy vrg-name]
```

Syntax Description

vrf name	(Optional) Enables VPN routing and forwarding (VRF) instance and VRF name.
global	(Optional) Configures a global routing table.
<i>address</i>	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
redundancy vrg-name	(Optional) Defines the VRG group name.

Defaults

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	The vrf name keyword and argument combination was added, and the global keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	The redundancy vrg-name keyword and argument combination was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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

Combined with the **ip forward-protocol** command, the **ip helper-address** command allows you to control which broadcast packets and which protocols are forwarded.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address should specify the address of the BOOTP or DHCP server. If you have multiple servers, you can configure one helper address for each server.

All of the following conditions must be met in order for a UDP or IP packet to be helpered by the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** command in global configuration mode.

If the DHCP server resides in a Virtual Private Network (VPN) or global space that is different from the interface VPN, then the **vrf name** or **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-address vrf name address** option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-address vrf name address** command is configured and later the vrf is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address address** command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf name address** command, then the previously configured **ip helper-address address** is considered to be global.



Note

The **ip helper-address** command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

Examples

The following example defines an address that acts as a helper address:

```
interface ethernet 1
 ip helper-address 10.24.43.2
```

The following example defines an address that acts as a helper address and is associated with the VRF named host1:

```
interface ethernet 1/0
 ip helper-address vrf host1 10.25.44.2
```

The following example defines an address that acts as a helper address and is associated with the VRG named group1:

```
interface ethernet 1/0
 ip helper-address 10.25.45.2 redundancy group1
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) unreachable messages are generated for a destination, use the **ip icmp rate-limit unreachable** command in global configuration mode. To use the default, use the **no** form of this command.

ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

no ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

Syntax Description

df	(Optional) Don't Fragment (DF) bit is set. The optional <i>ms</i> argument is a time limit in milliseconds (ms) in which one unreachable message is generated. If the df keyword is specified, its <i>ms</i> argument remains independent from those of general destination unreachable messages. The valid range is from 1 ms to 4294967295 ms. Note Counting begins as soon as this command is configured.
log	(Optional) Logging of generated messages that show packets that could not reach a destination at a specified threshold. The optional <i>packets</i> argument specifies a packet threshold. When it is reached, a log message is generated on the console. The default is 1000 packets. The optional <i>interval-ms</i> argument is a time limit for the interval for which a logging message is triggered. The default is 60000 ms, which is 1 minute.

Defaults

The default value is one ICMP destination unreachable message per 500 ms.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.4(2)T	The <i>packets</i> and the <i>interval-ms</i> arguments and log keyword were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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

Counting of packets begins when the command is configured and a packet threshold is specified.

The **no ip icmp rate-limit unreachable** command turns off the previously configured rate limit. To reset the rate limit to its default value, use the **ip icmp rate-limit unreachable** command default.

Cisco IOS software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **df** option is not configured, the **ip icmp rate-limit unreachable** command sets the time values in ms for DF destination unreachable messages.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 ms:

```
ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
no ip icmp rate-limit unreachable
```

The following example sets the rate limit back to the default:

```
no ip icmp rate-limit unreachable
```

The following example sets a logging packet threshold and time interval:

```
ip icmp rate-limit unreachable log 1200 120000
```

Related Commands

Command	Description
clear ip icmp rate-limit	Clears all ICMP unreachable destination messages or all statistics for a specified interface.
show ip icmp rate-limit	Displays all ICMP unreachable destination messages or all statistics for a specified interface.

ip icmp redirect

To control the type of Internet Control Message Protocol (ICMP) redirect message that is sent by the Cisco IOS software, use the **ip icmp redirect** command in global configuration mode. To set the value back to the default, use the **no** form of this command.

ip icmp redirect [host | subnet]

no ip icmp redirect [host | subnet]

Syntax Description

host	(Optional) Sends ICMP host redirects.
subnet	(Optional) Sends ICMP subnet redirects.

Defaults

The router will send ICMP subnet redirect messages.

Because the **ip icmp redirect subnet** command is the default, the command will not be displayed in the configuration.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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

An ICMP redirect message can be generated by a router when a packet is received and transmitted on the same interface. In this situation, the router will forward the original packet and send a ICMP redirect message back to the sender of the original packet. This behavior allows the sender to bypass the router and forward future packets directly to the destination (or a router closer to the destination).

There are two types of ICMP redirect messages: redirect for a host address or redirect for an entire subnet.

The **ip icmp redirect** command determines the type of ICMP redirects sent by the system and is configured on a per system basis. Some hosts do not understand ICMP subnet redirects and need the router to send out ICMP host redirects. Use the **ip icmp redirect host** command to have the router send out ICMP host redirects. Use the **ip icmp redirect subnet** command to set the value back to the default, which is to send subnet redirects.

To prevent the router from sending ICMP redirects, use the **no ip redirects** interface configuration command.

Examples

The following example enables the router to send out ICMP host redirects:

```
ip icmp redirect host
```

The following example sets the value back to the default, which is subnet redirects:

```
ip icmp redirect subnet
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages.

ip information-reply

To have the Cisco IOS software send Internet Control Message Protocol (ICMP) information replies, use the **ip information-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip information-reply

no ip information-reply

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.2T	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 ability for the Cisco IOS software to respond to ICMP information request messages with an ICMP information reply message is disabled by default. Use this command to allow the software to send ICMP information reply messages.

Examples

The following example enables the sending of ICMP information reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 10.108.1.0 255.255.255.0
 ip information-reply
```

ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** command in interface configuration mode. To disable IRDP routing, use the **no** form of this command.

ip irdp [**multicast** | **holdtime** *seconds* | **maxadvertinterval** *seconds* | **minadvertinterval** *seconds* | **preference** *number* | **address** *address* [*number*]]

no ip irdp

Syntax Description		
multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.	
holdtime <i>seconds</i>	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the maxadvertinterval value. Must be greater than maxadvertinterval and cannot be greater than 9000 seconds.	
maxadvertinterval <i>seconds</i>	(Optional) Maximum interval in seconds between advertisements. The range is from 1 to 1800. A value of 0 means only advertise when solicited. The default is 600 seconds.	
minadvertinterval <i>seconds</i>	(Optional) Minimum interval in seconds between advertisements. The range is from 1 to 1800. The default is 450 seconds.	
preference <i>number</i>	(Optional) Preference value. The allowed range is -2^{31} to 2^{31} . The default is 0. A higher value increases the preference level of the router. You can modify a particular router so that it will be the preferred router to which other routers will home.	
address <i>address</i> [<i>number</i>]	(Optional) IP address (<i>address</i>) to proxy advertise, and optionally, its preference value (<i>number</i>).	

Defaults

Disabled

When enabled, IRDP uses these defaults:

- Broadcast IRDP advertisements
- Maximum interval between advertisements: 600 seconds
- Minimum interval between advertisements: 450 seconds
- Preference: 0

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
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

If you change the **maxadvertinterval** value, the other two values also change, so it is important to change the **maxadvertinterval** value before changing either the **holdtime** or **minadvertinterval** values. The **ip irdp multicast** command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.

Examples

The following example sets the various IRDP processes:

```
!Enable irdp on interface Ethernet 0.

interface ethernet 0
 ip irdp

!Send IRDP advertisements to the multicast address.

 ip irdp multicast

!Increase router preference from 0 to 900.

 ip irdp preference 900

!Set maximum time between advertisements to 400 secs.

 ip irdp maxadvertinterval 400

!Set minimum time between advertisements to 100 secs.

 ip irdp minadvertinterval 100

!Advertisements are good for 6000 seconds.

 ip irdp holdtime 6000

!Proxy-advertise 10.108.14.5 with default router preference.

 ip irdp address 10.108.14.5

!Proxy-advertise 10.108.14.6 with preference of 50.

 ip irdp address 10.108.14.6 50
```

Related Commands

Command	Description
show ip irdp	Displays IRDP values.

ip mask-reply

To have the Cisco IOS software respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ip mask-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip mask-reply

no ip mask-reply

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration (config-if)

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.

Examples The following example enables the sending of ICMP mask reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 10.108.1.0 255.255.255.0
 ip mask-reply
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description

bytes MTU in bytes.

Defaults

Minimum is 128 bytes; maximum depends on the interface medium.

Command Modes

Interface configuration (config-if)

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

If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it. All devices on a physical medium must have the same protocol MTU in order to operate.



Note

Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

Examples

The following example sets the maximum IP packet size for the first serial interface to 300 bytes:

```
interface serial 0
 ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

ip redirects

To enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ip redirects

no ip redirects

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Interface configuration (config-if)

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 Previously, if the Hot Standby Router Protocol (HSRP) was configured on an interface, ICMP redirect messages were disabled by default for the interface. With Cisco IOS Release 12.1(3)T, ICMP redirect messages are enabled by default if HSRP is configured.

Examples The following example enables the sending of ICMP redirect messages on Ethernet interface 0:

```
interface ethernet 0
 ip redirects
```

Related Commands	Command	Description
	ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
	show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip sctp asconf

To enable the ability of an existing Stream Control Transmission Protocol (SCTP) endpoint to automatically send Address Configuration Change (ASCONF) chunks in response to an IP address change on a router without an authentication check, use the **ip sctp asconf** command in global configuration mode. To disable the requirement for ASCONF and ASCONF Acknowledgement (ASCONF-ACK) chunks to perform an authentication requirement check, use the **no** form of this command.

```
ip sctp asconf {authenticate check | auto}
```

```
no ip sctp asconf {authenticate check | auto}
```

Syntax Description

authenticate check	Configures SCTP to check that authentication is supported on the endpoint before sending an ASCONF chunk.
auto	Configures SCTP to automatically send ASCONF chunks in response to an IP address change on a router.

Command Default

SCTP checks the authentication status of the endpoint before sending an ASCONF chunk in response to an IP address change on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The ASCONF chunk format requires the receiving SCTP to not report to the sender if it does not understand the ASCONF chunk. This command enables you to configure sending the ASCONF chunk automatically in response to an IP address change in an SCTP stream, or to authenticate the endpoint before sending the ASCONF chunk.

The ASCONF chunk is used to communicate to the endpoint of an SCTP stream that at least one of the configuration change requests in the stream must be acknowledged.

Examples

The following example shows how to configure SCTP to authenticate the endpoint before sending an ASCONF chunk:

```
Router(config)# ip sctp asconf authenticate check
```

The following example shows how to configure SCTP to automatically send an ASCONF chunk in response to a change in the IP address of the remote endpoint:

```
Router(config)# ip sctp asconf auto
```

Related Commands

Command	Description
ip sctp authenticate	To define Stream Control Transmission Protocol (SCTP) data chunks that the client requires be authenticated.

ip sctp authenticate

To define Stream Control Transmission Protocol (SCTP) data chunks that the client requires be authenticated, use the **ip sctp authenticate** command in global configuration mode. To disable the authentication of an SCTP data chunk, use the **no** form of this command.

ip sctp authenticate {*chunk-type* | *chunk-number*}

no ip sctp authenticate {*chunk-type* | *chunk-number*}

Syntax Description

<i>chunk-type</i>	Name of the chunk type to be authenticated. See Table 1 in the “Usage Guidelines” section for a list of chunk types.
<i>chunk-number</i>	Number of the chunk to be authenticated in the range from 0 to 255.

Command Default

SCTP data chunks are not authenticated by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	This command was enhanced to support the Address Configuration (ASCONF) and ASCONF-ACK SCTP chunk types.

Usage Guidelines

SCTP Authentication procedures use either Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1), which can be memory and CPU intensive. Enabling SCTP Authentication on data chunks could impact CPU utilization when a large number of authenticated chunks are sent.

You cannot disable the authentication of the ASCONF or ASCONF-ACK chunks.

Enabling the authentication of a chunk type applies only to new endpoints and associations.

[Table 8](#) provides a list of SCTP chunk types and SCTP chunk numbers.

Table 8 SCTP Authentication Chunk Types

SCTP Chunk Type	SCTP Chunk Number	Description
abort association	0x06	ABORT chunk.
asconf	0xC1	ASCONF chunk.
asconf-ack	0x80	ASCONF acknowledgement chunk.
cookie-ack	0x0b	COOKIE acknowledgment chunk.
cookie-echo	0x0a	COOKIE-ECHO chunk.
data	0x00	DATA chunk.

Table 8 SCTP Authentication Chunk Types

SCTP Chunk Type	SCTP Chunk Number	Description
fwd-tsn	0xc0	FWD-CUM-TSN chunk. Forwarded cumulative transmission sequence number chunk.
heartbeat	0x04	HEARTBEAT request chunk.
heartbeat-ack	0x05	HEARTBEAT acknowledgement chunk.
packet-drop	0x81	PACKET-DROP chunk.
sack	0x03	Selective acknowledgment chunk.
shutdown	0x07	SHUTDOWN chunk.
shutdown-ack	0x08	SHUTDOWN acknowledgement chunk.
stream-reset	0x82	STREAM-RESET chunk.

Examples

The following example shows how to enable authentication of SCTP data chunks:

```
ip sctp authenticate data
```

Related Commands

Command	Description
show sctp association	Displays accumulated information for a specific SCTP association.
show sctp errors	Displays the error counts logged by SCTP.
show sctp statistics	Displays the overall statistics counts for SCTP activity.

ip slb capp udp

To enable the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enter SLB Content Application Peering Protocol (CAPP) configuration mode, use the **ip slb capp udp** command in global configuration mode. To disable the KAL-AP agent feature, use the **no** form of this command.

ip slb capp udp

no ip slb capp udp

Syntax Description This command has no arguments or keywords.

Defaults The KAL-AP agent is not enabled.

Command Modes Global configuration (config)

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

Examples The following example enables the KAL-AP agent and enters CAPP UDP configuration mode:

```
Router(config)# ip slb capp udp
```

Related Commands	Command	Description
	farm-weight	Specifies a weight to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when calculating the load value for a server farm.
	kal-ap domain	Specifies a domain tag to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when searching for a server farm.
	peer port	Specifies the port to which the IOS SLB KeepAlive Application Protocol (KAL-AP) agent is to connect.
	peer secret	Enables Message Digest Algorithm Version 5 (MD5) authentication for the IOS SLB KeepAlive Application Protocol (KAL-AP) agent.

ip slb dfp

To configure Dynamic Feedback Protocol (DFP), supply an optional password, and enter DFP configuration mode, use the **ip slb dfp** command in global configuration mode. To remove the DFP configuration, use the **no** form of this command.

```
ip slb dfp [password [encrypt] secret-string [timeout]]
```

```
no ip slb dfp
```

Syntax Description	
password	(Optional) Password for Message Digest Algorithm Version 5 (MD5) authentication.
<i>encrypt</i>	(Optional) Indicates how the <i>secret-string</i> 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 : <ul style="list-style-type: none"> 0—The <i>secret-string</i> is stored in plain text. This is the default setting. 7—The <i>secret-string</i> is encrypted before it is displayed or written to nonvolatile memory. <p>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.</p>
<i>secret-string</i>	(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 <i>secret-string</i> is always sent in plain text when the configuration is downloaded. The <i>secret-string</i> must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
<i>timeout</i>	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The valid range is 0 to 65535 seconds. The default value is 180 seconds, if a password is specified.

Defaults

The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds, if a password is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.

Release	Modification
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(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 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.

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 to allow enough time for you to update the password on all agents and servers before the timeout expires. Setting a longer timeout 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, the password must match the one specified on the **password** command in DFP agent configuration mode in the DFP agent.

Examples

The following example configures DFP, sets the DFP password to Password1 and the timeout to 360 seconds, and enters DFP configuration mode:

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

Related Commands

Command	Description
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and enters DFP agent configuration mode.

ip slb entries

To configure an initial allocation and a maximum value for IOS Server Load Balancing (IOS SLB) database entries, use the **ip slb entries** command in global configuration mode. To restore the default values, use the **no** form of this command.

```
ip slb entries [conn [init-conn [max-conn]] | frag [init-frag [max-frag] | lifetime timeout] | gtp {gsn
init-gsn [max-gsn] | nsapi init-nsapi [max-nsapi] | sticky [init-sticky [max-sticky]]]
```

```
no ip slb entries [conn | frag [lifetime] | gtp {gsn | nsapi} | sticky]
```

Syntax	Description
conn	(Optional) Configures an initial allocation and a maximum value for IOS SLB connection database entries.
<i>init-conn</i>	(Optional) Initial allocation of connection database entries. When the number of available entries is reduced to less than half of the <i>init-conn</i> argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the <i>max-conn</i> argument. Valid range is 1 to 1000000 connection database entries. The default is 8000 connection database entries. Note Be careful when setting the <i>init-conn</i> argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
<i>max-conn</i>	(Optional) Maximum number of connection database entries that can be allocated. Valid range is 1 to 8000000 connection database entries. The default is 8000000 connection database entries.
frag	(Optional) Configures an initial allocation and a maximum value for IOS SLB fragment database entries.
<i>init-frag</i>	(Optional) Initial allocation of routing entries in the fragment database. When the number of available entries is reduced to less than half of the <i>init-frag</i> argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the <i>max-frag</i> argument. Valid range is 1 to 1000000 connection database entries. The default is 2000 connection database entries. Note Be careful when setting the <i>init-frag</i> argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
<i>max-frag</i>	(Optional) Maximum number of fragment database entries that can be allocated. Valid range is 1 to 8000000 fragment database entries. The default is 32000 fragment database entries.

lifetime <i>timeout</i>	(Optional) Lifetime of an entry in the IOS SLB fragment database, in seconds. Valid range is 1 to 255 seconds. The default value is 10 seconds.
gtp	(Optional) Configures an initial allocation and a maximum value for IOS SLB general packet radio service (GPRS) Tunneling Protocol (GTP) database entries.
gsn	(Optional) Configures an initial allocation and a maximum value for IOS SLB GPRS support node (GSN) database entries.
<i>init-gsn</i>	(Optional) Initial allocation of GSN database entries. When the number of available entries is reduced to less than half of the <i>init-gsn</i> argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the <i>max-gsn</i> argument. Valid range is 1 to 5000 GSN database entries. The default is 200 GSN database entries. Note Be careful when setting the <i>init-gsn</i> argument to a very high value, such as 5000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 500.
<i>max-gsn</i>	(Optional) Maximum number of GSN database entries that can be allocated. Valid range is 1 to 20000 GSN database entries. The default is 20000 GSN database entries.
nsapi	(Optional) Configures an initial allocation and a maximum value for IOS SLB Network Service Access Point Identifier (NSAPI) database entries.
<i>init-nsapi</i>	(Optional) Initial allocation of NSAPI database entries. When the number of available entries is reduced to less than half of the <i>init-nsapi</i> argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the <i>max-nsapi</i> argument. Valid range is 1 to 1000000 NSAPI database entries. The default is 8000 NSAPI database entries. Note Be careful when setting the <i>init-nsapi</i> argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
<i>max-nsapi</i>	(Optional) Maximum number of NSAPI database entries that can be allocated. Valid range is 1 to 8000000 NSAPI database entries. The default is 8000000 NSAPI database entries.
sticky	(Optional) Configures an initial allocation and a maximum value for IOS SLB sticky connection database entries.

<i>init-sticky</i>	<p>(Optional) Initial allocation of sticky database entries. When the number of available entries is reduced to less than half of the <i>init-sticky</i> argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the <i>max-sticky</i> argument.</p> <p>Valid range is 1 to 1000000 sticky database entries. The default is 4000 sticky database entries.</p> <p>Note Be careful when setting the <i>init-sticky</i> argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.</p>
<i>max-sticky</i>	<p>(Optional) Maximum number of sticky database entries that can be allocated. Valid range is 1 to 8000000 sticky database entries. The default is 8000000 sticky database entries.</p>

Defaults

For the connection database, the default initial allocation is 8000 connections, and the default maximum is 8000000 connections.

For the fragment database, the default initial allocation is 2000 fragments, and the default maximum is 8000000 fragments. The default lifetime is 10 seconds.

For the GSN database, the default initial allocation is 200 GSNs, and the default maximum is 20000 GSNs.

For the NSAPI database, the default initial allocation is 8000 NSAPIs, and the default maximum is 8000000 NSAPIs.

For the sticky connection database, the default initial allocation is 4000 sticky connections, and the default maximum is 3200 sticky connections.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(11b)E	The lifetime keyword and <i>timeout</i> argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The gsn , gtp , and nsapi keywords and <i>init-gsn</i> , <i>init-nsapi</i> , <i>max-gsn</i> , and <i>max-nsapi</i> arguments 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

Enter this command *before* entering the rest of your IOS SLB configuration. If you have already begun configuring IOS SLB before entering this command, you must reload IOS SLB after entering this command.

If you configure an initial allocation value that exceeds the amount of available memory, memory might not be available for other features. In extreme cases, the router or switch might not boot properly. Therefore, be careful when you configure initial allocation values.

Examples

The following example configures an initial allocation of 128,000 connections, which can grow dynamically to a limit of 512,000 connections:

```
Router(config)# ip slb entries conn 128000 512000
```

Related Commands

Command	Description
show ip slb conns	Displays all connections handled by IOS SLB, or, optionally, only those connections associated with a particular virtual server or client.

ip slb firewallfarm

To identify a firewall farm and enter firewall farm configuration mode, use the **ip slb firewallfarm** command in global configuration mode. To remove the firewall farm from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

ip slb firewallfarm *firewall-farm*

no ip slb firewallfarm *firewall-farm*

Syntax Description	<i>firewall-farm</i>	Character string used to identify the firewall farm. The character string is limited to 15 characters.
---------------------------	----------------------	--

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

Command Modes	Global configuration (config)
----------------------	-------------------------------

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	Grouping real servers into firewall farms is an essential part of IOS SLB firewall load balancing. Using firewall farms enables IOS SLB to assign new connections to the real servers based on their weighted capacities, and on the load-balancing algorithms used.
-------------------------	--

Examples	The following example identifies a firewall farm named FIRE1:
-----------------	---

```
Router(config)# ip slb firewallfarm FIRE1
```

Related Commands	Command	Description
	real (firewall farm)	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.

ip slb map

To configure an IOS SLB protocol map and enter SLB map configuration mode, use the **ip slb map** command in global configuration mode. To delete the map, use the **no** form of this command.

```
ip slb map map-id {gtp | radius}
```

```
no ip slb map map-id {gtp | radius}
```

Syntax Description		
<i>map-id</i>		IOS SLB protocol map identifier. The valid range is from 1 to 255.
gtp		For general packet radio service (GPRS) load balancing, configures an IOS SLB GPRS Tunneling Protocol (GTP) map and enters SLB GTP map configuration mode.
radius		For RADIUS load balancing, configures an IOS SLB RADIUS map and enters SLB RADIUS map configuration mode.

Defaults None

Command Modes Global configuration (config)

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

Usage Guidelines

You can configure up to 255 IOS SLB GTP or RADIUS maps. However, we recommend that you configure no more than 10 maps for a given virtual server.

Each map ID must be unique across all server farms associated with a given GTP or RADIUS virtual server. That is, you cannot configure more than one map with the same ID.

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

Configure the **gtp** or **radius** keyword only on maps that are to be used with GTP or RADIUS virtual servers, respectively.

Examples

The following example configures IOS SLB RADIUS map 1 and enters SLB RADIUS map configuration mode:

```
Router(config)# ip slb map 1 radius
```

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.
show ip slb map	Displays information about IOS SLB protocol maps.
username (IOS SLB)	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

ip slb maxbuffers frag

To configure the maximum number of buffers for the IOS Server Load Balancing (IOS SLB) fragment database, use the **ip slb maxbuffers frag** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip slb maxbuffers frag *buffers*

no ip slb maxbuffers frag

Syntax Description

buffers

Maximum number of out-of-order trailing fragments to be buffered simultaneously in the IOS SLB fragment database, waiting for the leader fragment. This value can help prevent IOS SLB memory from being overrun in the event of a fragment attack.

Valid range is 0 to 65535 buffers. The default value is 100 buffers.

Defaults

The default maximum is 100 buffers.

Command Modes

Global configuration (config)

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 sets the maximum number of buffers for the IOS SLB fragment buffer to 300:

```
Router(config)# ip slb maxbuffers frag 300
```

ip slb natpool

To configure an IOS Server Load Balancing (IOS SLB) Network Address Translation (NAT) to create at least one client address pool, use the **ip slb natpool** command in global configuration mode. To remove an **ip slb natpool** configuration, use the **no** form of this command.

```
ip slb natpool pool start-ip end-ip [netmask netmask | prefix-length leading-1-bits] [entries
init-address [max-address]]
```

```
no ip slb natpool pool
```

Syntax	Description
<i>pool</i>	Character string used to identify this client address pool. The character string is limited to 15 characters.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
netmask <i>netmask</i>	(Optional) Configures the mask for the associated IP subnet. Specifies the netmask of the network to which the pool addresses belong.
prefix-length <i>leading-1-bits</i>	(Optional) Specifies how many bits of the netmask are ones (that is, how many bits of the address indicate the network).
entries	(Optional) Configures an initial allocation and optional maximum value for IOS SLB client NAT address entries for the <i>pool</i> argument.
<i>init-address</i>	(Optional) Initial allocation of client NAT address entries. The number of client NAT address entries can grow dynamically: When the number of available client NAT address entries is less than half of the <i>init-address</i> argument, IOS SLB allocates additional client NAT address entries. Valid range is 1 to 1000000 client NAT address entries. The default is 8000 client NAT address entries.
<i>max-address</i>	(Optional) Maximum number of client NAT address entries that can be allocated. Valid range is 1 to 8000000 client NAT address entries. The default is the maximum number of ports that can be allocated within the IP address range specified for <i>pool</i> . For example, the following command: <pre>ip slb natpool 10.1.10.1 10.1.10.5 prefix-length 24 entries 8000</pre> has a default <i>max-address</i> of (10.1.10.1-10.1.10.1.5*54535, or 4*54535, or 218140.

Defaults

The default initial allocation is 8000 client NAT address entries.

The default maximum number of client NAT address entries that can be allocated is the maximum number of ports that can be allocated within the IP address range.

Command Modes Global configuration (config)

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 If you want to use client NAT, you must create at least one client address pool.

The range of IP addresses in the address pool, configured with the *start-ip* and *end-ip* arguments, must not overlap the IP address for a VLAN as specified on the **ip address** interface configuration command.

Examples

The following example configures an IOS SLB NAT server farm pool of addresses with the name `web-clients`, the IP address range from 10.1.10.1 to 10.1.10.5, and a subnet mask of 255.255.0.0:

```
Router(config)# ip slb natpool web-clients 10.1.10.1 10.1.10.5 netmask 255.255.0.0
```

Related Commands

Command	Description
show ip slb natpool	Displays information about the IOS SLB NAT configuration.
show ip slb serverfarms	Displays information about the server farm configuration.