ip slb probe custom udp

To configure a custom User Datagram Protocol (UDP) probe name and enter custom UDP probe configuration mode, use the **ip slb probe custom udp** command in global configuration mode. To remove a custom UDP probe name, use the **no** form of this command.

ip slb probe *probe* **custom udp**

no ip slb probe *probe*

Syntax Description

probe	Name of the custom UDP probe. The character string is limited to 15 characters.

Defaults

No custom UDP probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the custom UDP probe name and application protocol and enters custom UDP configuration mode.

The custom UDP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE6, then enters custom UDP probe configuration mode:

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

Related Commands

Command	Description
address (custom UDP probe)	Configures an IP address to which to send custom UDP probes.
interval (custom UDP probe)	Configures a custom UDP probe interval.
port (custom UDP probe)	Specifies the port to which a custom UDP probe is to connect.
request (custom UDP probe)	Defines the payload of the UDP request packet to be sent by a custom UDP probe.
response	Defines the data string to match against custom UDP probe response packets.
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe dns

To configure a Domain Name System (DNS) probe name and enter DNS probe configuration mode, use the **ip slb probe dns** command in global configuration mode. To remove a DNS probe name, use the **no** form of this command.

ip slb probe *probe* **dns**

no ip slb probe *probe*

Syntax Description

probe	Name of the DNS probe. The character string is limited to 15 characters.

Defaults

No DNS probe is configured.

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.

Usage Guidelines

DNS probes send domain name resolve requests to real servers and verify the returned IP addresses.

This command configures the DNS probe name and application protocol and enters DNS configuration mode.

The DNS probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE4, then enters DNS probe configuration mode:

```
Router(config)# ip slb probe PROBE4 dns
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe http

To configure an HTTP probe name and enter HTTP probe configuration mode, use the **ip slb probe http** command in global configuration mode. To remove an HTTP probe name, use the **no** form of this command.

ip slb probe *probe* **http**

no ip slb probe *probe*

Syntax Description

probe	Name of the HTTP probe. The character string is limited to 15 characters.

Defaults

No HTTP probe is configured.

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

This command configures the HTTP probe name and application protocol and enters HTTP configuration mode.

The HTTP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Note HTTP probes require a route to the virtual server. The route is not used, but it must exist to enable the sockets code to verify that the destination can be reached, which in turn is essential for HTTP probes to function correctly. The route can be either a host route (advertised by the virtual server) or a default route (specified using the **ip route 0.0.0.0 0.0.0.0** command, for example).

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE2, then enters HTTP probe configuration mode:

```
Router(config)# ip slb probe PROBE2 http
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe ping

To configure a ping probe name and enter ping probe configuration mode, use the **ip slb probe ping** command in global configuration mode. To remove a ping probe name, use the **no** form of this command.

ip slb probe *probe* **ping**

no ip slb probe *probe*

Syntax Description

probe	Name of the ping probe. The character string is limited to 15 characters.

Defaults

No ping probe is configured.

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

This command configures the ping probe name and application protocol and enters ping configuration mode.

The ping probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE1, then enters ping probe configuration mode:

```
Router(config)# ip slb probe PROBE1 ping
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe tcp

To configure a TCP probe name and enter TCP probe configuration mode, use the **ip slb probe tcp** command in global configuration mode. To remove a TCP probe name, use the **no** form of this command.

ip slb probe *probe* **tcp**

no ip slb probe *probe*

Syntax Description

probe	Name of the TCP probe. The character string is limited to 15 characters.

Defaults

No TCP probe is configured.

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.

Usage Guidelines

This command configures the TCP probe name and application protocol and enters TCP configuration mode.

The TCP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE5, then enters TCP probe configuration mode:

```
Router(config)# ip slb probe PROBE5 tcp
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe wsp

To configure a Wireless Session Protocol (WSP) probe name and enter WSP probe configuration mode, use the **ip slb probe wsp** command in global configuration mode. To remove a WSP probe name, use the **no** form of this command.

ip slb probe *probe* **wsp**

no ip slb probe *probe*

Syntax Description

probe	Name of the WSP probe. The character string is limited to 15 characters.

Defaults

No WSP probe is configured.

Command Modes

Global configuration (config)

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.

Usage Guidelines

This command configures the WSP probe name and application protocol and enters WSP probe configuration mode.

The WSP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE3, then enters WSP probe configuration mode:

```
Router(config)# ip slb probe PROBE3 wsp
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb replicate slave rate

To set the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication, use the **ip slb replicate slave rate** command in global configuration mode. To restore the default rate, use the **no** form of this command.

ip slb replicate slave rate *rate*

no ip slb replicate slave rate *rate*

Syntax Description

rate	Replication message rate for IOS SLB slave replication, in messages per second. The valid range is 50 messages per second to 1000 messages per second. The default setting is 400 messages per second.

Defaults

The default rate is 400 messages per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables you to manage Interprocess Communication Channel (IPC) resources between two route processors. If there is congestion between the two route processors, use this command to set a lower rate.

If the replication rate is exceeded, IOS SLB issues an appropriate error message.

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

The Home Agent Director does not support the **ip slb replicate slave rate** command in global configuration mode.

Examples

The following example sets the replication message rate to 500 messages per second:

```
Router(config)# ip slb replicate slave rate 500
```

Related Commands

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

ip slb route

To enable IOS Server Load Balancing (IOS SLB) to route packets using the RADIUS framed-IP sticky database, or to route packets from one firewall real server back through another firewall real server, use the **ip slb route** command in global configuration mode. To route packets normally, use the **no** form of this command.

ip slb route {**framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**}

no ip slb route {**framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**}

Syntax Description

framed-ip deny	(Optional) Packets that do not match entries in the IOS SLB RADIUS framed-ip sticky database are not routed.
ip-address	(Optional) IP address of packets to be inspected.
netmask	(Optional) Subnet mask specifying a range of packets to be inspected.
framed-ip	(Optional) Packets are to be routed using the IOS SLB RADIUS framed-IP sticky database.
inter-firewall	(Optional) Enables IOS SLB to route packets from one firewall real server back through another firewall real server, if the flows to the destination IP would otherwise have been firewall load-balanced. This can be done within the same firewall farm or across different firewall farms.

Defaults

Cisco IOS SLB cannot route packets using the RADIUS framed-IP sticky database, nor can it route packets from one firewall real server back through another firewall real server.

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.
12.1(13)E3	The **inter-firewall** keyword was added.
12.2 (14)ZA6	The **framed-ip deny** keyword was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables IOS SLB to inspect packets whose source IP addresses match the specified IP address and subnet mask. IOS SLB then searches for the packet's source IP address in the RADIUS framed-IP sticky database. If the database contains a matching entry, IOS SLB routes the packet to the associated real server. If the database does not contain a matching entry, IOS SLB routes the packet normally.

The **inter-firewall** keyword is useful when traffic is arriving from an address behind a firewall, is destined for an address behind a firewall, and has a sticky entry to be routed via the routing table.

Examples

The following example enables IOS SLB to inspect packets with the source IP address 10.10.10.1:

```
Router(config)# ip slb route 10.10.10.1 255.255.255.255 framed-ip
```

Related Commands

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

ip slb serverfarm

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

ip slb serverfarm *server-farm*

no ip slb serverfarm *server-farm*

Syntax Description

server-farm	Character string used to identify the server farm. The character string is limited to 15 characters.

Defaults

No server farm is identified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Grouping real servers into server farms is an essential part of IOS SLB. Using server 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 server farm named PUBLIC:

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

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.

ip slb static

To configure a real server's Network Address Translation (NAT) behavior and enter static NAT configuration mode, use the **ip slb static** command in global configuration mode. To restore the real server's default NAT behavior, use the **no** form of this command.

ip slb static {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}}

no ip slb static {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}}

Syntax Description

drop	Indicates that IOS Server Load Balancing (IOS SLB) is to drop packets from this real server if the packets do not correspond to existing connections. This option is usually used in conjunction with the subnet mask or port number option on the **real** command in static NAT configuration mode, such that IOS SLB builds connections to the specified subnet or port, and drops all other connections from the real server.
nat virtual	Configures the real server to use server NAT, and to use the virtual IP address that is configured on the **real** command in static NAT configuration mode when translating addresses.
nat *virtual-ip*	Configures the real server to use server NAT, and to use the specified virtual IP address when translating addresses.
per-packet	(Optional) IOS SLB is *not* to maintain connection state for packets originating from the real server. That is, IOS SLB is to use server NAT to redirect packets originating from the real server.
sticky	(Optional) Indicates that IOS SLB is *not* to maintain connection state for packets originating from the real server, *unless* those packets match a sticky object. That is, if IOS SLB can find a matching sticky object, it builds the connection. Otherwise, IOS SLB does not build the connection.

Defaults

If you do not specify either the **per-packet** or **sticky** keyword, IOS SLB maintains connection state for packets originating from the real server.

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.

Usage Guidelines

If you specify the *virtual-ip* argument and you do not specify the **per-packet** option, IOS SLB uses server port translation to distinguish between connection requests initiated by different real servers.

Examples

The following example specifies that the real server is to use server NAT and to use virtual IP address 10.1.10.1 when translating addresses, and that IOS SLB is not to maintain connection state for any packets originating from the real server:

```
Router(config)# ip slb static nat 10.1.10.1 per-packet
```

Related Commands

Command	Description
show ip slb static	Displays information about the static NAT configuration.

ip slb timers gtp gsn

To change the amount of time IOS Server Load Balancing (IOS SLB) maintains sessions to and from an idle gateway general packet radio service (GPRS) support node (GGSN) or serving GPRS support node (SGSN), use the **ip slb timers gtp gsn** command in global configuration mode. To restore the default GPRS support node (GSN) idle timer, use the **no** form of this command.

ip slb timers gtp gsn *duration*

no ip slb timers gtp gsn *duration*

Syntax Description

duration	GSN idle timer duration in seconds, which defines how long IOS SLB is to allow a GGSN or SGSN to be idle (that is, to go without echoing or signaling through IOS SLB). When the timer expires, IOS SLB cleans up all sessions that are using the idle GGSN or SGSN. The valid range is 1 to 65535 seconds. The default value is 90 seconds.

Defaults

The default duration is 90 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command sets the GSN idle timer for all IOS SLB virtual servers that are configured for GPRS Tunneling Protocol (GTP) cause code inspection. When the GSN idle timer expires, IOS SLB destroys all sessions to and from the idle GGSN or SGSN.

Examples

The following example specifies that IOS SLB maintains sessions for 45 seconds after a GGSN or SGSN becomes idle:

```
Router(config)# ip slb timers gtp gsn 45
```

Related Commands

Command	Description
virtual	Configures the virtual server attributes.

ip slb vserver

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

ip slb vserver *virtual-server*

no ip slb vserver *virtual-server*

Syntax Description

virtual-server	Character string used to identify the virtual server. The character string is limited to 15 characters.

Defaults

No virtual server is identified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example identifies a virtual server named PUBLIC_HTTP:

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

Related Commands

Command	Description
serverfarm	Associates a real server farm with a virtual server, and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets going through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss *max-segment-size*

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Command Default

The MSS is determined by the originating host.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was changed from **ip adjust-mss** to **ip tcp adjust-mss**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZU2	This command was integrated into Cisco IOS Release 12.2(18)ZU2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes.

The PPP over Ethernet (PPPoE) standard supports an MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the Internet Control Message Protocol (ICMP) error messages that must be relayed from the host in order for path MTU to work.

The **ip tcp adjust-mss** command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The **ip tcp adjust-mss** command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the **ip mtu** command on the same interface as the **ip tcp adjust-mss** command, we recommend that you use the following commands and values:

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

Examples

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1.255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
 pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list permit ip 192.168.100.0.0.0.0.255 any
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

ip tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp chunk-size *characters*

no ip tcp chunk-size

Syntax Description

characters	Maximum number of characters that Telnet or rlogin can read in one read instruction. The default value is 0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.

Defaults

0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.1	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

It is unlikely you will need to change the default value.

Examples

The following example sets the maximum TCP read size to 64,000 bytes:

```
ip tcp chunk-size 64000
```

ip tcp compression-connections

To specify the total number of Transmission Control Protocol (TCP) header compression connections that can exist on an interface, use the **ip tcp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections

Syntax Description

number	Number of TCP header compression connections the cache supports, in the range from 3 to 256.

Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable).
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

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

Note Both ends of the serial connection must use the same number of cache entries.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

Related Commands

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

ip tcp ecn

To enable TCP Explicit Congestion Notification (ECN), use the **ip tcp ecn** command in global configuration mode. To disable TCP ECN, use the **no** form of this command.

ip tcp ecn

no ip tcp ecn

Syntax Description

This command has no arguments or keywords.

Command Default

TCP ECN is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following example shows how to enable TCP ECN:

```
ip tcp ecn
```

Related Commands

Command	Description
debug ip tcp ecn	Turns on TCP ECN debugging.
show tcp tcb	Displays the status of local and remote end hosts.

ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode. To disable compression, use the **no** form of this command.

ip tcp header-compression [**passive | iphc-format | ietf-format**]

no ip tcp header-compression [**passive | iphc-format | ietf-format**]

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.

Command Default

Disabled

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links.*

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. This command was modified to include the **ietf-format** keyword.
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

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other protocol headers.

The passive Keyword

By default, the **ip tcp header-compression** command compresses outgoing TCP traffic. If you specify the **passive** keyword, outgoing TCP traffic is compressed only if incoming TCP traffic on the same interface is compressed. If you do not specify the **passive** keyword, all outgoing TCP traffic is compressed.

For PPP interfaces, the **passive** keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Real-Time Transport Protocol (RTP) header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

The ietf-format Keyword

The **ietf-format** keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the **ietf-format** keyword compresses only TCP packets. For PPP interfaces, when the **ietf-format** keyword is specified, RTP header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format** keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
Router(config-if)# end
```

Related Commands

Command	Description
ip tcp compression-connections	Specifies the total number of TCP header compression connections that can exist on an interface.
show ip tcp header-compression	Displays TCP/IP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss** command in global configuration mode. To disable the configuration of the MSS, use the no form of this command.

ip tcp mss *bytes*

no ip tcp mss *bytes*

Syntax Description

bytes	Maximum segment size for TCP connections in bytes. Valid values are from 68 to 10000.

Defaults

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(05)S	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
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 this command is not enabled, the MSS value of 536 bytes is used if the destination is not on a LAN, otherwise the MSS value is 1460 for a local destination.

For connections originating from a router, the specified value is used directly as an MSS option in the synchronize (SYN) segment. For connections terminating on a router, the value is used only if the incoming SYN segment has an MSS option value higher than the configured value. Otherwise the incoming value is used as the MSS option in the SYN/acknowledge (ACK) segment.

Note The **ip tcp mss** command interacts with the **ip tcp path-mtu-discovery** command and not the **ip tcp header-compression** command. The **ip tcp path-mtu-discovery** command changes the default MSS to 1460 even for nonlocal nodes.

Examples

The following example sets the MSS value at 250:

```
ip tcp mss 250
```

Related Commands

Command	Description
ip tcp header-compression	Specifies the total number of header compression connections that can exist on an interface.

ip tcp path-mtu-discovery

To enable the Path MTU Discovery feature for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** command in global configuration mode. To disable the function, use the **no** form of this command.

ip tcp path-mtu-discovery [**age-timer** {*minutes* | **infinite**}]

no ip tcp path-mtu-discovery [**age-timer** {*minutes* | **infinite**}]

Syntax Description

age-timer *minutes*	(Optional) Time interval (in minutes) after which TCP re-estimates the path MTU with a larger maximum segment size (MSS). The maximum is 30 minutes; the default is 10 minutes.
age-timer infinite	(Optional) Turns off the age timer.

Defaults

Disabled. If enabled, the minutes default is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.2	The **age-timer** and **infinite** keywords were 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

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection. It is described in RFC 1191. Existing connections are not affected when this feature is turned on or off.

Customers using TCP connections to move bulk data between systems on distinct subnets would benefit most by enabling this feature.

The age timer is a time interval for how often TCP reestimates the path MTU with a larger MSS. When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You can turn off the age timer by setting it to infinite.

Examples

The following example enables Path MTU Discovery:

```
ip tcp path-mtu-discovery
```

ip tcp queuemax

To alter the maximum TCP outgoing queue per connection, use the **ip tcp queuemax** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp queuemax *packets*

no ip tcp queuemax

Syntax Description

packets	Outgoing queue size of TCP packets. The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.

Defaults

The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.

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

Changing the default value changes the 5 segments, not the 20 segments.

Examples

The following example sets the maximum TCP outgoing queue to 10 packets:

```
ip tcp queuemax 10
```

ip tcp selective-ack

To enable TCP selective acknowledgment, use the **ip tcp selective-ack** command in global configuration mode. To disable TCP selective acknowledgment, use the **no** form of this command.

ip tcp selective-ack

no ip tcp selective-ack

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 F	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

TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round-trip time. An aggressive sender could resend packets early, but such re-sent segments might have already been received.

The TCP selective acknowledgment mechanism helps overcome these limitations. The receiving TCP returns selective acknowledgment packets to the sender, informing the sender about data that has been received. The sender can then resend only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when a multiple number of packets drop from a TCP window. There is no performance impact when the feature is enabled but not used.

This command becomes effective only on new TCP connections opened after the feature is enabled.

This feature must be disabled if you want TCP header compression. You might disable this feature if you have severe TCP problems.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

Examples

The following example enables the router to send and receive TCP selective acknowledgments:

```
ip tcp selective-ack
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

ip tcp synwait-time

To set a period of time the Cisco IOS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** command in global configuration mode. To restore the default time, use the **no** form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Syntax Description

seconds	Time (in seconds) the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.

Defaults

The default time is 30 seconds.

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

In versions previous to Cisco IOS software Release 10.0, the system would wait a fixed 30 seconds when attempting to establish a TCP connection. If your network contains public switched telephone network (PSTN) dial-on-demand routing (DDR), the call setup time may exceed 30 seconds. This amount of time is not sufficient in networks that have dialup asynchronous connections because it will affect your ability to Telnet over the link (from the router) if the link must be brought up. If you have this type of network, you may want to set this value to the UNIX value of 75.

Because this is a host parameter, it does not pertain to traffic going *through* the router, just for traffic originated *at* this device. Because UNIX has a fixed 75-second timeout, hosts are unlikely to experience this problem.

Examples

The following example configures the Cisco IOS software to continue attempting to establish a TCP connection for 180 seconds:

```
ip tcp synwait-time 180
```

ip tcp timestamp

To enable TCP time stamp, use the **ip tcp timestamp** command in global configuration mode. To disable TCP time stamp, use the **no** form of this command.

ip tcp timestamp

no ip tcp timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	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

TCP time stamp improves round-trip time estimates. Refer to RFC 1323 for more detailed information on TCP time stamp.

The TCP time stamp must be disabled if you want to use TCP header compression.

Examples

The following example enables the router to send TCP time stamps:

```
ip tcp timestamp
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

ip tcp window-size

To alter the TCP window size, use the **ip tcp window-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp window-size *bytes*

no ip tcp window-size

Syntax Description

bytes	Window size (in bytes). An integer from 0 to 1073741823. The default value is 4128 bytes. Window scaling is enabled when the window size is greater than 65535 bytes.

Command Default

The default window size is 4128 bytes when window scaling is not enabled. If only one neighbor is configured for the window scaling extension, the default window size is 65535 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.1	This command was introduced.
12.2(8)T	Default window size and maximum window scaling factor were increased.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

To enable window scaling to support Long Fat Networks (LFNs), the TCP window size must be more than 65,535 bytes. The remote side of the link also needs to be configured to support window scaling. If both sides are not configured with window scaling, the default maximum value of 65,535 bytes is applied.

The scale factor is automatically calculated based on the window-size you configure. You cannot directly configure the scale factor.

Examples

The following example shows how to set the TCP window size to 1000 bytes:

```
ip tcp window-size 1000
```

ip unreachables

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachables** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip unreachables

no ip unreachables

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

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects all types of ICMP unreachable messages.

Examples

The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ip unreachables
```

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf (tracking)

To track an IP route in a specific VPN virtual routing and forwarding (VRF) table, use the **ip vrf** command in tracking configuration mode. To remove the tracking of the route, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

The tracking of a route is not configured.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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

This command is available for all IP-route tracked objects that are tracked by the **track ip route** global configuration command. Use this command to track a route that belongs to a specific VPN.

Examples

In the following example, the route associated with a VRF named VRF1 is tracked:

```
track 1 ip route 10.0.0.0 255.0.0.0 metric threshold
 ip vrf VRF1
 rd 100:1
 route-target both 100:1
!
interface e0/2
 no shutdown
 ip vrf forwarding VRF1
 ip address 10.0.0.2 255.0.0.0
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VPN VRF with an interface or subinterface.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

ip wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*}[**accelerated**] [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0**-**7**] *password*]

no ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*}[**accelerated**] [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0**-**7**] *password*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Specifies the web-cache service (WCCP version 1 and version 2). **Note** Web cache counts as one service. The maximum number of services, including those assigned with the *service-number* argument, are 256.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword. **Note** If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
accelerated	(Optiona) Enables hardware acceleration.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
open	(Optional) Identifies the service as open. This is the default service mode.
closed	(Optional) Identifies the service as closed.
group-address *multicast-address*	(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which web cache should receive redirected messages.
redirect-list *access-list*	(Optional) Access list that controls traffic redirected to this service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list *access-list*	(Optional) Access list that determines which web caches are allowed to participate in the service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password [**0**-**7**] *password*	(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be any value between 0 and 7 (inclusive), with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default WCCP services are not enabled on the router.

Command Modes Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command replaced the **ip wccp enable**, **ip wccp redirect-list**, and **ip wccp group-list** commands.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The maximum value for the *service-number* argument was increased to 254.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **service-list** *service-access-list* keyword and argument pair and the **mode open** and **mode closed** keywords were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.

Usage Guidelines WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching should be enabled on the content engine interface, and the **ip wccp web-cache redirect out** command should be specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

This command instructs a router to enable or disable the support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a vrf to associate with a service group. You can then specify a web-cache service name or service number.

The same service (web-cache or service number) can be configured in different VRF tables. Each service will operate independently.

When the **no ip wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*} **group-address** *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all "Here I Am" messages are responded to with a unicast reply.

ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*} **redirect-list** *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- User Datagram Protocol (UDP) (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic will prevent the web caches from ever seeing the packets that are intercepted.

ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*} **group-list** *access-list*

This option instructs the router to use an access list to control the web caches allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.

Note The **ip wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ip wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ip wccp group-listen** command in the *Cisco IOS IP Application Services Command Reference*.

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

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

ip wccp *service-number* **service-list** *service-access-list* **mode closed**

In applications where the interception and redirection of WCCP packet flows to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, it is necessary to block packet flows for the application when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client
10.1.1.13
```

When there is a conflict in service list definitions, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
ip multicast-routing
ip wccp 99 group-address 239.0.0.0
interface ethernet 0
 ip wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
access-list 100 deny ip any host 10.168.196.51
access-list 100 permit ip any any
ip wccp web-cache redirect-list 100
interface ethernet 0
 ip wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
ip wccp web-cache
ip wccp check acl outbound
interface fastethernet0/0
 ip access-group 10 out
 ip wccp web-cache redirect out
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

The following example shows how to configure a closed WCCP service:

```
ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP you wish to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp check acl outbound

To check the outbound access control list (ACL) for Web Cache Communication Protocol (WCCP), use the **ip wccp check acl outbound** command in global configuration mode. To disable the outbound check, use the **no** form of this command.

ip wccp check acl outbound

no ip wccp check acl outbound

Syntax Description

This command has no arguments or keywords.

Defaults

Check of the outbound ACL services is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to configure a router to run WCCP a check of outbound ACLs:

```
ip wccp check acl outbound
```

Related Commands

Command	Description
ip wccp	Allocates space and enables support of the WCCP service group.
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP to use on a router.

ip wccp check services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ip wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ip wccp check services all

no ip wccp check services all

Syntax Description

This command has no arguments or keywords.

Defaults

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

With the **ip wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL as well as by the priority value of the service.

It is possble to configure an interface with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found which matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check servies all** command is configured. When the **ip wccp check services all** command is configred, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

Note The priority of a WCCP service group is determined by the web cache appliance. The priority of a WCCP service group cannot be configured via Cisco IOS.

Note The **ip wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples

The following example shows how to configure all WCCP services:

```
ip wccp check services all
```

Related Commands

Command	Description
ip wccp	Allocates space and enables support of specified WCCP services for participation in a service group.
ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp enable

The **ip wccp enable** command has been replaced by the **ip wccp** command. See the description of the **ip wccp** command in this chapter for more information.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP), use the **ip wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

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

no ip wccp [**vrf** *vrf-name*] {**web-cache** | *service number*} **group-listen**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Directs the router to send packets to the web cache service.
service-number	WCCP service number; valid values are from 0 to 254.

Defaults

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Note To ensure correct operation on Catalyst 6500 series switches and Cisco 7600 series routers, you must enter the **ip pim** *mode* command in addition to the **ip wccp group-listen** command.

On Cisco 7600 series routers, the *service-number* may be either one of the provided standard keyword definitions or a number representing a cache engine dynamically defined definition. Once the service is enabled, the router can participate in the establishment of a service group.

On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- Configure the IP multicast address for use by the WCCP Service Group.
- Enable IP multicast routing using the **ip multicast-routing** command in global configuration mode.
- Configure the interfaces on which the router wishes to receive the IP multicast address with the **ip wccp** {**web-cache** | *service-number*} **group-listen** interface configuration command.

Examples

The following example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100.

```
Router# configure terminal
Router(config)# ip multicast-routing
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache group-listen
```

Related Commands

Command	Description
ip wccp	Directs a router to enable or disable the support for a WCCP cache engine service group.
ip wccp redirect	Enables WCCP redirection on an interface.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

no ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Enables the web-cache service.
service-number	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Redirection checking on the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(11)S	The **in** keyword was added.
12.1(3)T	The **in** keyword was added.
12.2(17d)SXB	Support for this command on the Cisco 7600 series router Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 720.
12.2(18)SXF	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tips Be careful not to confuse the **ip wccp redirect** {**out** | **in**} interface configuration command with the **ip wccp redirect exclude in** interface configuration command.

Note This command has the potential to affect the **ip wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the "exclude in" command will be overridden. The opposite is also true: configuring the "exclude in" command will override the "redirect in" command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when fast/CEF switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ip address 10.21.21.1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ip nat outside
Router(config-if)# ip inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP statistics.

ip wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ip wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description

This command has no arguments or keywords.

Defaults

Redirection exclusion is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check that may occur at the outbound interface. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the internet as well as allow for the use of the Web Cache Communication Protocol (WCCP) v2 packet return feature.

Examples

In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
interface ethernet 0
 ip wccp redirect exclude in
```

Related Commands

Command	Description
ip wccp	Directs a router to enable or disable the support for a cache engine service group.
ip wccp redirect out	Configures an interface to enable a the ability of a router to verify that appropriate packets are being redirected to a cache engine.

ip wccp redirect-list

This command is now documented as part of the **ip wccp** command. See the description of the **ip wccp** command in this book for more information.

ip wccp version

To specify the version of Web Cache Communication Protocol (WCCP), use the **ip wccp version** command in global configuration mode.

ip wccp version {**1** | **2**}

Syntax Description

1	Web Cache Communication Protocol Version 1 (WCCPv1).
2	Web Cache Communication Protocol Version 2 (WCCPv2).

Defaults

WCCPv2

Command Modes

Global configuration (config)

Command History

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

Examples

In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
Router(config)# ip wccp version 1

Router# show ip wccp

% WCCP version 2 is not enabled
```

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated [[**group-address** *group-address*] | [**redirect-list** *access-list*] | [**group-list** *access-list*] | [**password** *password*]]

no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This command is supported on software releases later than cache engine software Release ACNS 4.2.1.

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages

that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access-list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access-list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

kal-ap domain

To enable the IOS SLB KeepAlive Application Protocol (KAL-AP) agent to look for a domain tag when reporting the load for a virtual server, use the **kal-ap domain** command in server farm configuration mode. To delete the domain tag, use the **no** form of this command.

kal-ap domain *tag*

no kal-ap domain

Syntax Description

tag	1- to 64-character domain tag to be used by the KAL-AP agent. All characters are valid; case is significant.

Defaults

The KAL-AP agent does not look for a domain tag when reporting the load for a virtual server.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

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

Usage Guidelines

Configure the **kal-ap domain** command on the server farm that is associated with the virtual server for which the KAL-AP agent is to report the load.

Examples

The following example specifies that the KAL-AP agent is to look for domain tag **chicago.com**:

```
Router(config-slb-sfarm)# kal-ap domain chicago-com
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.
ip slb serverfarm	Identifies a server farm and enter SLB server farm configuration mode.