ip tcp adjust-mss through ip wccp web-cache accelerated

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets that go 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 modified. 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, the host 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 size is 1460 bytes, when the default MTU of the containing IP datagram 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 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 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 that pass through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value and the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte IP datagram that matches the MTU size of 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 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
access-list 101 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.

Command Default

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:

```
Router(config)# 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:

```
Router(config)# 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

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 keepalive

To configure TCP keepalive parameters, use the **ip tcp keepalive** command in global configuration mode. To restore the default configuration, use the **no** form of this command.

ip tcp keepalive {**interval** *seconds*| **retries** *retry-number*}

no ip tcp keepalive

Syntax Description

interval *seconds*	Specifies the TCP keepalive interval in seconds. The range is from 1 to 7200. The default value is 60 seconds.
retries *retry-number*	Specifies the number of TCP keepalive retries. The range is from 1 to 10. The default value is 4.

Command Default

TCP keepalive parameters are configured with their default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

- This command can be used only on TTY and vty applications.
- The keepalive probing can be enabled by configuring the **service tcp-keepalives-in** and **service tcp-keepalives-out** commands. However, the parameters of the **ip tcp keepalive** command can be modified without configuring these commands.

Examples

The following example shows how to set the TCP keepalive interval as 23:

```
Device# configure terminal
Device(config)# ip tcp keepalive interval 23
```

Related Commands

Command	Description
configure replace	Replaces the current running configuration with a saved Cisco IOS configuration file.
service tcp-keepalives-in	Generates keepalive packets on the idle incoming network connection.
services tcp-keepalives-out	Generates keepalive packets on the idle outgoing network connections.

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.

Command Default

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:

```
Router(config)# 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.

Command Default

Path MTU Discovery is 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:

```
Router(config)# 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.

Command Default

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:

```
Router(config)# 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.

Command Default

TCP selective acknowledgment is not enabled.

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:

```
Router(config)# 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.

Command Default

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:

```
Router(config)# 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.

Command Default

TCP time stamp is 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:

```
Router(config)# 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 window size, 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. Window scaling is enabled when the window size is greater than 65535 bytes. **Note** As of Cisco IOS Release 15.0(1)M, the *bytes* argument can be set to an integer from 68 to 1073741823.

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.
15.0(1)M	This command was modified. The valid window size (in bytes) was changed to 68 to 1073741823.

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 that you configure. You cannot directly configure the scale factor.

Examples

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

```
Router(config)# 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.

Command Default

ICMP unreachable messages are not 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:

```
Router(config)# interface ethernet 0
Router(config-if)# 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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

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

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# 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 or IPv6 route in a specific VPN virtual routing and forwarding (VRF) table, use the **ip vrf** or **ipv6 vrf** command in tracking configuration mode. To remove the tracking of the route, use the **no** form of this command.

{**ip**| **ipv6**} **vrf** *vrf-name*

no {**ip**| **ipv6**} **vrf** *vrf-name*

Syntax Description

ip	Tracks an IP route.
ipv6	Tracks an IPv6 route.
vrf-name	Name assigned to a VRF.

Command Default

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.
15.3(3)M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

This command is available for all IP-route or IPv6 -route tracked objects that are tracked by the **track route** command in global configuration mode. Use this command to track a route that belongs to a specific VPN.

Examples

In the following example, the route associated with the VRF1 table is tracked:

```
Router(config)# track 1 ip route 10.0.0.0 255.0.0.0 metric threshold
Router(config-track)# ip vrf VRF1
Router(config-track)# rd 100:1
```

```
Router(config-track)# route-target both 100:1
!
Router(config)# interface ethernet0/2
Router(config-if)# no shutdown
Router(config-if)# ip vrf forwarding VRF1
Router(config-if)# ip address 10.0.0.2 255.0.0.0
```

In the following example, the IPv6 route associated with the VRF2 table is tracked:

```
Router(config)# track 6 ipv6 route 2001:DB8:0:ABCD::1/10 metric threshold
Router(config-track)# ipv6 vrf VRF2
```

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 is one of the services. The maximum number of services, including those assigned with the *service-number* argument, is 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 used in the cache cluster, the reverse proxy service is indicated by a value of 99.
accelerated	(Optional) This option applies only to hardware-accelerated routers. This keyword configures the service group to prevent a connection being formed with a cache engine unless the cache engine is configured in a way that allows redirection on the router to benefit from hardware acceleration.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
mode open	(Optional) Identifies the service as open. This is the default service mode.
mode closed	(Optional) Identifies the service as closed.

group-address *multicast-address*	(Optional) Specifies the 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) Specifies the 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) in length that specifies the access list.
group-list *access-list*	(Optional) Specifies the access list that determines which web caches are allowed to participate in the service group. The *access-list* argument specifies either the number or the name of a standard or extended access list.
password [**0** | **7**] *password*	(Optional) Specifies the 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 0 or 7, 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.

Release	Modification
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.
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. 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. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a router to enable or disable 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 also sent to the group address. 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 the number or the name of a standard or extended 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:

- 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 that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named 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 in length. 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 packets to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, packets for the application must be blocked 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 be used only 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 the 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 service list definitions conflict, 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:

```
Router(config)# ip multicast-routing
Router(config)# ip wccp 99 group-address 239.0.0.0
Router(config)# interface ethernet 0
Router(config-if)# 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:

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface ethernet 0
Router(config-if)# 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 access control list (ACL) check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config-if)# 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:

```
Router(config)# ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp group listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for WCCP.
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.

Command	Description
ip wccp version	Specifies which version of WCCP you want to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp check acl outbound

To check the access control list (ACL) for egress interfaces for packets redirected by the Web Cache Communication Protocol (WCCP), use the **ip wccp check acl outbound** command in global configuration mode. To disable the outbound check for redirected packets, 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.

Command Default

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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command performs the same function as the **ip wccp outbound-acl-check** command.

Examples

The following example shows how to configure a router to check the ACL for the egress interfaces for inbound packets that are redirected by WCCP:

```
Router(config)# ip wccp check acl outbound
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ip wccp check services all	Enables all WCCP services.
ip wccp outbound-acl-check	Checks the ACL for egress interfaces for packets redirected by WCCP.
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.

Command Default

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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

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 access control list (ACL) and by the priority value of the service.

An interface can be configured 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 that 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 services all** command is configured. When the **ip wccp check services all** command is configured, 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 software.

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:

```
Router(config)# ip wccp check services all
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ip wccp version	Specifies which version of WCCP you want 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 (VRF) instance 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.

Command Default

No interface is configured to enable the reception of IP multicast packets for WCCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB	Support was added for the Supervisor Engine 2.
12.2(18)SXD1	Support was added for 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.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelin

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 value for the *service-number* argument 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.

Note the following requirements on routers that are to be members of a service group when IP multicast is used:

- 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 wants 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 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 multicast-routing	Enables IP multicast routing.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables WCCP redirection on an interface.
ipv6 multicast-routing	Enables multicast routing.

ip wccp outbound-acl-check

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

ip wccp outbound-acl-check

no ip wccp outbound-acl-check

Syntax Description

This command has no arguments or keywords.

Command Default

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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command performs the same function as the **ip wccp check acl outbound** command.

Examples

The following example shows how to configure a router to check the ACL for the egress interfaces for inbound packets that are redirected by WCCP:

```
Router(config)# ip wccp outbound-acl-check
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp check acl outbound	Checks the ACL for egress interfaces for packets redirected by WCCP.
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP to use on a router.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using the 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 (VRF) instance 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 was added for the Cisco 7600 series router Supervisor Engine 2.
12.2(18)SXD1	Support was added for the Cisco 7600 series router Supervisor Engine 720.

Release	Modification
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. **Note** The **out** keyword is not supported in 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.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** keyword and *vrf-name* argument were added. Support for the **out** keyword was added.
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding on the content engine interface, and specify the **ip wccp web-cache redirect out** command. 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. 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. Packets that match the criteria will be redirected.

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

Tip 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 can affect the **ip wccp redirect exclude in** command behavior. (These commands have opposite functions.) If you have the **ip wccp redirect exclude in** command set on an interface and you subsequently configure the **ip wccp redirect in** command, the **ip wccp redirect exclude in** command will be overridden. The opposite is also true: Configuring the **ip wccp redirect exclude in** command will override the **ip wccp redirect in** command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when Cisco Express Forwarding 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	Enables support of the specified WCCP service for participation in a service group.
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 global configuration and 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.

Command Default

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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check. 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 and to allow for the use of the WCCPv2 packet return feature.

Examples

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

```
Router(config)# interface ethernet 0
Router(config-if)# ip wccp redirect exclude in
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.

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 source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ip wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] **source-interface** *source-interface*

no ip wccp [**vrf** *vrf-name*] **source-interface**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
source-interface	The type and number of the source interface.

Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID. If a loopback interface does not exist, then the interface that WCCP uses as the preferred router ID and GRE source address cannot be specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv4 address.

The interface identified by the *source-interface* argument must be assigned an IPv4 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, the configuration is ignored and a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface
 ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch** --The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist** --The interface has been deleted.
- **no address** --The interface does not have a valid IPv4 address.
- **line protocol down** --The interface is not fully operational.

In the error case above, the source interface for the router ID will be selected automatically.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol ("Here I Am" and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

Examples

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ip wccp source-interface gigabitethernet0/0/0
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.

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

Command Default

WCCPv2 is enabled.

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.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. Only WCCP version 2 is supported in Cisco IOS XE Release 2.2.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Configuring this command does not have any impact on Cisco ASR 1000 Series Aggregation Services Routers because these routers support only WCCPv2. WCCPv2 is enabled by default on Cisco ASR 1000 Series Aggregation Services Routers when a service group is configured or a service group is attached to an interface.

Examples

In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1:

```
Router(config)# ip wccp version 1
Router# show ip wccp
% WCCP version 2 is not enabled
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.

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.

Command Default

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

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.

Usage Guidelines

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.