ip mtu

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

ip mtu *bytes*

no ip mtu

Syntax Description

bytes	MTU in bytes.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it.

All devices on a physical medium must have the same protocol MTU in order to operate.

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

Examples

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

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

Related Commands

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

ip redirects

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

ip redirects

no ip redirects

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
interface ethernet 0
 ip redirects
```

Related Commands

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

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** global configuration command. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** global configuration command. 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

Command History

Release	Modification
9.1	This command was introduced.

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 TCP header compression connections that can exist on an interface, use the **ip tcp compression-connections** interface configuration command. To restore the default, use the **no** form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections *number*

Syntax Description

number	Number of TCP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).

Defaults

The default number is 32 connections.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay, PPP, and High-Level Data Link Control (HDLC) encapsulation, the maximum number of compression connections increased to 256. For Frame Relay, the maximum value is fixed, not configurable.

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:

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands

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

ip tcp header-compression

To enable TCP header compression, use the **ip tcp header-compression** interface configuration command. To disable compression, use the **no** form of this command.

ip tcp header-compression [**passive**]

no ip tcp header-compression [**passive**]

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, the Cisco IOS software compresses all traffic.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

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. RFC 1144 specifies the compression process. 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 UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This condition means that fast interfaces like T1 can overload the router. Consider the traffic characteristics of your network before using this command.

Examples

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

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands

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

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 *mss-value*

no ip tcp mss *mss-value*

Syntax Description

mss-value	Maximum segment size for TCP connections in bytes. The range is from 68 to 10000.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(05)S	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.

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 non-local 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** global configuration command. 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 default *minutes* value is 10 minutes.

Command Modes

Global configuration

Command History

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

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 re-estimates 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** global configuration command. 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

Command History

Release	Modification
10.0	This command was introduced.

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** global configuration command. 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

Command History

Release	Modification
11.2 F	This command was introduced.

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** global configuration command. 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

Command History

Release	Modification
10.0	This command was introduced.

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 might 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** global configuration command. 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

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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

This feature 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** global configuration command. 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). The maximum is 65,535 bytes. The default value is 2144 bytes.

Defaults

The default size is 2144 bytes.

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.

Usage Guidelines

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

If your TCP window size is set to 1000 bytes, for example, you could have 1 packet of 1000 bytes or 2 packets of 500 bytes, and so on. However, there is also a limit on the number of packets allowed in the window. There can be a maximum of 5 packets if the connection has TTY; otherwise there can be 20 packets.

Examples

The following example sets 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** interface configuration command. 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

Command History

Release	Modification
10.0	This command was introduced.

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
```

permit (IP)

To set conditions for a named IP access list, use the **permit** access-list configuration command. To remove a condition from an access list, use the **no** form of this command.

permit *source* [*source-wildcard*]

no permit *source* [*source-wildcard*]

permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

no permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

permit icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Group Management Protocol (IGMP)

For IGMP, you can also use the following syntax:

permit igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

permit tcp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol UDP)

For UDP, you can also use the following syntax:

permit udp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines" of the **access-list** (IP extended) command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.

port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11) and 12.1(2)	The **fragments** keyword was added.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

The **time-range** option allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access-list entry is applied only to noninitial fragments. **Note** The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where

there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.5.34.0  0.0.0.255
 permit 128.88.0.0  0.0.255.255
 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
```

Related Commands

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access list entry, up to 100 characters long.

Defaults

The access list entries have no remarks.

Command Modes

Standard named or extended named access-list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the Jones subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow Jones subnet to telnet out
 deny tcp host 171.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

show access-lists

To display the contents of current access lists, use the **show access-lists** privileged EXEC command.

show access-lists [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

The system displays all access lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(5)T	The command output was modified to identify compiled access lists.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command

```
Router# show access-lists
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

For information on how to configure access lists, refer to the "Configuring IP Services" chapter of the *Cisco IOS IP Configuration Guide*.

For information on how to configure dynamic access lists, refer to the "Traffic Filtering and Firewalls" chapter of the *Cisco IOS Security Configuration Guide*.

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of all current IP access lists.

show access-list compiled

To display a table showing Turbo Access Control Lists (ACLs), use the **show access-list compiled** EXEC command.

show access-list compiled

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

Examples

The following is a partial sample output of the **show access-list compiled** command:

```
Router# show access-list compiled

Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
 ACL         State      Tables  Entries  Config  Fragment  Redundant  Memory
1           Operational    1        2        1         0          0      1Kb
2           Operational    1        3        2         0          0      1Kb
3           Operational    1        4        3         0          0      1Kb
4           Operational    1        3        2         0          0      1Kb
5           Operational    1        5        4         0          0      1Kb
9           Operational    1        3        2         0          0      1Kb
20          Operational    1        9        8         0          0      1Kb
21          Operational    1        5        4         0          0      1Kb
101         Operational    1       15        9         7          2      1Kb
102         Operational    1       13        6         6          0      1Kb
120         Operational    1        2        1         0          0      1Kb
199         Operational    1        4        3         0          0      1Kb
First level lookup tables:
Block      Use              Rows       Columns   Memory used
  0   TOS/Protocol            6/16      12/16      66048
  1   IP Source (MS)         10/16      12/16      66048
  2   IP Source (LS)         27/32      12/16      132096
  3   IP Dest (MS)            3/16      12/16      66048
  4   IP Dest (LS)            9/16      12/16      66048
```

```
5   TCP/UDP Src Port         1/16     12/16      66048
6   TCP/UDP Dest Port        3/16     12/16      66048
7   TCP Flags/Fragment       3/16     12/16      66048
```

Related Commands

Command	Description
access-list compiled	Enables the Turbo ACL feature.
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Creates a standard access list.
clear access-list counters	Clears the counters of an access list.
clear access-temp	Manually clears a temporary access list entry from a dynamic access list.
ip access-list	Defines an IP access list by name.
show ip access-list	Displays the contents of all current IP access lists.

show interface mac

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

show interface [*type number*] **mac**

Syntax Description

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

The **show interface mac** command displays information for all interfaces configured for MAC accounting. To display information for a single interface, use the **show interface** *type number* **mac** command.

For incoming packets on the interface, the accounting statistics are gathered before the CAR/DCAR feature is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after output CAR, before output DCAR or DWRED or DWFQ feature is performed on the packet. Therefore, if a you are using DCAR or DWRED on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command because the calculations are done prior to the features.

The maximum number of MAC addresses that can be stored for the input address is 512 and the maximum number of MAC address that can be stored for the output address is 512. After the maximum is reached, subsequent MAC addresses are ignored.

To clear the accounting statistics, use the **clear counter** EXEC command. To configure an interface for IP accounting based on the MAC address, use the **ip accounting mac-address** interface configuration command.

Examples

The following is sample output from the **show interface mac** command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent.

```
Router# show interface ethernet 0/1/1 mac
Ethernet0/1/1
  Input  (511 free)
    0007.f618.4449(228):  4 packets, 456 bytes, last: 2684ms ago
                  Total:  4 packets, 456 bytes
  Output  (511 free)
    0007.f618.4449(228):  4 packets, 456 bytes, last: 2692ms ago
                  Total:  4 packets, 456 bytes
```

Related Commands

Command	Description
ip accounting mac-address	Enables IP accounting on any interface based on the source and destination MAC address.

show interface precedence

To display precedence accounting information for interfaces configured for precedence accounting, use the **show interface precedence** EXEC command.

show interface [*type number*] **precedence**

Syntax Description

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

The **show interface precedence** command displays information for all interfaces configured for IP precedence accounting. To display information for a single interface, use the **show interface** *type number* **precedence** command.

For incoming packets on the interface, the accounting statistics are gathered before input CAR/DCAR is performed on the packet. Therefore, if CAR/DCAR changes the precedence on the packet, it is counted based on the old precedence setting with the **show interface precedence** command.

For outgoing packets on the interface, the accounting statistics are gathered after output DCAR or DWRED or DWFQ feature is performed on the packet.

To clear the accounting statistics, use the **clear counter** EXEC command.

To configure an interface for IP accounting based on IP precedence, use the **ip accounting precedence** interface configuration command.

Examples

The following is sample output from the **show interface precedence** command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.

```
Router# show interface ethernet 0/1/1 precedence
Ethernet0/1/1
  Input
    Precedence 0:  4 packets, 456 bytes
  Output
    Precedence 0:  4 packets, 456 bytes
```

Related Commands

Command	Description
ip accounting precedence	Enables IP accounting on any interface based on IP precedence.

show ip access-list

To display the contents of all current IP access lists, use the **show ip access-list** EXEC command.

show ip access-list [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

Displays all standard and extended IP access lists.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-list** command when all access lists are requested:

```
Router# show ip access-list

Extended IP access list 101
   deny udp any any eq ntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter

Extended IP access list Internetfilter
   permit tcp any 171.69.0.0 0.0.255.255 eq telnet
   deny tcp any any
   deny udp any 171.69.0.0 0.0.255.255 lt 1024
   deny ip any any log
```

show ip accounting

To display the active accounting or checkpointed database or to display access list violations, use the **show ip accounting** EXEC command.

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

Syntax Description

checkpoint	(Optional) Indicates that the checkpointed database should be displayed.
output-packets	(Optional) Indicates that information pertaining to packets that passed access control and were routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.
access-violations	(Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.

Defaults

If neither the **output-packets** nor **access-violations** keyword is specified, the **show ip accounting** command displays information pertaining to packets that passed access control and were routed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **access-violations** and **output-packet** keywords were added.

Usage Guidelines

If you do not specify any keywords, the **show ip accounting** command displays information about the active accounting database, and traffic coming from a remote site and transiting through a router.

To display IP access violations, you must use the **access-violations** keyword. If you do not specify the keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

To use this command, you must first enable IP accounting on a per-interface basis.

Examples

The following is sample output from the **show ip accounting** command:

```
Router# show ip accounting

   Source           Destination              Packets               Bytes
 131.108.19.40    192.67.67.20                   7                 306
 131.108.13.55    192.67.67.20                  67                2749
 131.108.2.50     192.12.33.51                  17                1111
 131.108.2.50     130.93.2.1                     5                 319
 131.108.2.50     130.93.1.2                   463               30991
 131.108.19.40    130.93.2.1                     4                 262
```

```
131.108.19.40    130.93.1.2                    28               2552
131.108.20.2     128.18.6.100                  39               2184
131.108.13.55    130.93.1.2                    35               3020
131.108.19.40    192.12.33.51                1986              95091
131.108.2.50     192.67.67.20                 233              14908
131.108.13.28    192.67.67.53                 390              24817
131.108.13.55    192.12.33.51              214669            9806659
131.108.13.111   128.18.6.23                27739            1126607
131.108.13.44    192.12.33.51               35412            1523980
192.31.7.21      130.93.1.2                    11                824
131.108.13.28    192.12.33.2                   21               1762
131.108.2.166    192.31.7.130                 797             141054
131.108.3.11     192.67.67.53                   4                246
192.31.7.21      192.12.33.51               15696             695635
192.31.7.24      192.67.67.20                  21                916
131.108.13.111   128.18.10.1                   16               1137
accounting threshold exceeded for 7 packets and 433 bytes
```

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
131.108.19.40    192.67.67.20             7          306         77
131.108.13.55    192.67.67.20            67         2749        185
131.108.2.50     192.12.33.51            17         1111        140
131.108.2.50     130.93.2.1               5          319        140
131.108.19.40    130.93.2.1               4          262         77

Accounting data age is 41
```

The following is sample output from the **show ip accounting** command. The output shows the original source and destination addresses that are separated by three routers:

```
Router3# show ip accounting

Source                  Destination             Packets                 Bytes
10.225.231.154          172.16.10.2             44                      28160
10.76.97.34             172.16.10.2             44                      28160
10.10.11.1              172.16.10.2             507                     324480
10.10.10.1              172.16.10.2             507                     318396
10.100.45.1             172.16.10.2             508                     325120
10.98.32.5              172.16.10.2             44                      28160

Accounting data age is 2
```

Table 17 describes the significant fields shown in the displays.

Table 17 show ip accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the **access-violations** keyword, the number of packets sent from the source address to the destination address that violated an Access Control List (ACL).

Table 17 show ip accounting Field Descriptions (continued)

Field	Description
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the **access-violations** keyword, the total number of bytes sent from the source address to the destination address that violated an ACL.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.

Related Commands

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

show ip casa affinities

To display statistics about affinities, use the **show ip casa affinities** EXEC command.

show ip casa affinities [**stats**] | [**saddr** *ip-address* [**detail**]] | [**daddr** *ip-address* [**detail**]] | **sport** *source-port* [**detail**]] | **dport** *destination-port* [**detail**]] | **protocol** *protocol* [**detail**]]

Syntax Description

stats	(Optional) Displays limited statistics.
saddr *ip-address*	(Optional) Displays the source address of a given TCP connection.
detail	(Optional) Displays the detailed statistics.
daddr *ip-address*	(Optional) Displays the destination address of a given TCP connection.
sport *source-port*	(Optional) Displays the source port of a given TCP connection.
dport *destination-port*	(Optional) Displays the destination port of a given TCP connection.
protocol *protocol*	(Optional) Displays the protocol of a given TCP connection.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
172.26.56.13    19    161.44.36.118   1118  TCP
```

The following is sample output of the **show ip casa affinities detail** command:

```
Router# show ip casa affinities detail

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0102 SYN FRAG
    Interest Tickle: 0x0005 FIN RST
    Dispatch (Layer 2):     YES               Dispatch Address: 172.26.56.33

Source Address  Port  Dest Address    Port  Prot
172.26.56.13    19    161.44.36.118   1118  TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0104 RST FRAG
    Interest Tickle: 0x0003 FIN SYN
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip casa affinities Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Port	Destination of a given TCP connection.
Prot	Protocol of a given TCP connection.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager address that is to receive interest packets for this affinity.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of TCP packet types that the services manager is interested in.
Interest Tickle	List of TCP packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the Forwarding Agent will listen for wildcard and fixed affinities.
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa oper

To display operational information about the Forwarding Agent, use the **show ip casa oper** EXEC command.

show ip casa oper

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 206.10.20.34/32
  Casa multicast address is 224.0.1.2
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip casa oper Field Descriptions

Field	Description
Casa is Active	The Forwarding Agent is active.
Casa control address	Unique address for this Forwarding Agent.
Casa multicast address	Services manager broadcast address.
Listening for wildcards on	Port on which the Forwarding Agent will listen.
Port	Services manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa stats

To display statistical information about the Forwarding Agent, use the **show ip casa stats** EXEC command.

show ip casa stats

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stats

Casa is active:
  Wildcard Stats:
    Wildcards:       6           Max Wildcards:    6
    Wildcard Denies: 0           Wildcard Drops:   0
    Pkts Throughput: 441         Bytes Throughput: 39120
  Affinity Stats:
    Affinities:      2           Max Affinities:   2
    Cache Hits:      444         Cache Misses:     0
    Affinity Drops:  0
  Casa Stats:
    Int Packet:      4           Int Tickle:       0
    Casa Denies:     0           Drop Count:       0
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip casa stats Field Descriptions

Field	Description
Casa is Active	The Forwarding Agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the Forwarding Agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.
Bytes Throughput	Number of bytes passed through all wildcards.
Affinity Stats	Affinity statistics.

Table 20 show ip casa stats Field Descriptions (continued)

Field	Description
Affinities	Current number of affinities.
Max Affinities	Maximum number of affinities since the forwarding agent became active.
Cache Hits	Number of packets that match wildcards and fixed affinities.
Cache Misses	Matched wildcard, missed fix.
Affinity Drops	Number of times an affinity could not be created.
Casa Stats	Forwarding agent statistics.
Int Packet	Interest packets.
Int Tickle	Interest tickles.
Casa Denies	Protocol violation.
Security Drops	Packets dropped due to password or authentication mismatch.
Drop Count	Number of messages dropped.

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa wildcard

To display information about wildcard blocks, use the **show ip casa wildcard** EXEC command.

show ip casa wildcard [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa wildcard** command:

```
Router# show ip casa wildcard

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     TCP
172.26.56.2     255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
172.26.56.13    255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
```

The following is sample output of the **show ip casa wildcard detail** command:

```
router# show ip casa wildcard detail

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x8000 ALLPKTS
    Interest Tickle: 0x0107 FIN SYN RST FRAG
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
    Advertise Dest Address: YES               Match Fragments:  NO

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
```

```
Interest Addr:          172.26.56.19      Interest Port: 1638
Interest Packet: 0x8102 SYN FRAG ALLPKTS
Interest Tickle: 0x0005 FIN RST
Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
Advertise Dest Address: YES               Match Fragments:  NO
```

Note If a filter is not set, the filter is not active.

Table 21 describes significant fields shown in the display.

Table 21 show ip casa wildcard Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Services manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	Does wildcard also match fragments? (boolean)

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** EXEC command.

show ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following is sample output from the **show ip drp** command:

```
Router# show ip drp

Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using "test" key-chain
```

Table 22 describes the significant fields shown in the display.

Table 22 show ip drp Field Descriptions

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.

show ip redirects

To display the address of a default gateway (router) and the address of hosts for which an Internet Control Message Protocol (ICMP) redirect message has been received, use the **show ip redirects** EXEC command.

show ip redirects

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command displays the default router (gateway) as configured by the **ip default-gateway** command.

The **ip mtu** command enables the router to send ICMP redirect messages.

Examples

The following is sample output from the **show ip redirects** command:

```
Router# show ip redirects

Default gateway is 160.89.80.29

Host               Gateway           Last Use    Total Uses  Interface
131.108.1.111      160.89.80.240         0:00             9  Ethernet0
128.95.1.4         160.89.80.240         0:00             4  Ethernet0
Router#
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
ip mtu	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

show ip sockets

To display IP socket information, use the **show ip sockets** command in privileged EXEC mode or user EXEC mode.

show ip sockets

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC
User EXEC

Command History

Release	Modification
10.0 T	This command was introduced.

Usage Guidelines

Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Examples

The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets

Proto    Remote       Port      Local          Port  In Out Stat TTY OutputIF
 17       0.0.0.0        0    171.68.186.193    67   0   0    1   0
 17   171.68.191.135  514    171.68.191.129  1811   0   0    0   0
 17   172.16.135.20   514    171.68.191.1    4125   0   0    0   0
 17   171.68.207.163   49    171.68.186.193    49   0   0    9   0
 17       0.0.0.0      123    171.68.186.193   123   0   0    1   0
 88       0.0.0.0        0    171.68.186.193   202   0   0    0   0
 17   172.16.96.59  32856    171.68.191.1     161   0   0    1   0
 17     --listen--             --any--        496   0   0    1   0
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip sockets Field Descriptions

Field	Description
Proto	Protocol number. For example, 17 is UDP, and 88 is EIGRP.
Remote	Remote address connected to this networking device. If the remote address is considered illegal, “--listen--” is displayed.
Port	Remote port. If the remote address is considered illegal, “--listen--” is displayed.
Local	Local address. If the local address is considered illegal or is the address 0.0.0.0, “--any--” displays.
Port	Local port.
In	Input queue size.
Out	Output queue size.
Stat	Various statistics for a socket.
TTY	The tty number for the creator of this socket.
OutputIF	Output IF string, if one exists.

show ip tcp header-compression

To display statistics about TCP header compression, use the **show ip tcp header-compression** EXEC command.

show ip tcp header-compression

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip tcp header-compression** command:

```
Router# show ip tcp header-compression

TCP/IP header compression statistics:
  Interface Serial1: (passive, compressing)
    Rcvd:    4060 total, 2891 compressed, 0 errors
             0 dropped, 1 buffer copies, 0 buffer failures
    Sent:    4284 total, 3224 compressed,
             105295 bytes saved, 661973 bytes sent
             1.15 efficiency improvement factor
    Connect: 16 slots, 1543 long searches, 2 misses, 99% hit ratio
             Five minute miss rate 0 misses/sec, 0 max misses/sec
```

Table 24 describes significant fields shown in the display.

Table 24 show ip tcp header-compression Field Descriptions

Field	Description
Rcvd:	
total	Total number of TCP packets received.
compressed	Total number of TCP packets compressed.
errors	Unknown packets.
dropped	Number of packets dropped due to invalid compression.
buffer copies	Number of packets that needed to be copied into bigger buffers for decompression.
buffer failures	Number of packets dropped due to a lack of buffers.
Sent:	
total	Total number of TCP packets sent.
compressed	Total number of TCP packets compressed.

Table 24 show ip tcp header-compression Field Descriptions (continued)

Field	Description
bytes saved	Number of bytes reduced.
bytes sent	Number of bytes sent.
efficiency improvement factor	Improvement in line efficiency because of TCP header compression.
Connect:	
slots	Size of the cache.
long searches	Indicates the number of times the software needed to look to find a match.
misses	Indicates the number of times a match could not be made. If your output shows a large miss rate, then the number of allowable simultaneous compression connections may be too low.
hit ratio	Percentage of times the software found a match and was able to compress the header.
Five minute miss rate	Calculates the miss rate over the previous 5 minutes for a longer-term (and more accurate) look at miss rate trends.
max misses/sec	Maximum value of the previous field.

Related Commands

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

show ip traffic

To display statistics about IP traffic, use the **show ip traffic** command in user EXEC or privileged EXEC mode.

show ip traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2	The output was enhanced to displays the number of keepalive, open, update, route-refresh request, and notification messages that have been received and sent by a Border Gateway Protocol (BGP) routing process.

Examples

The following is sample output from the **show ip traffic** command:

```
Router# show ip traffic

IP statistics:
  Rcvd:  2961 total, 2952 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 9 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 9 received, 36 sent
  Mcast: 2294 received, 2293 sent
  Sent:  2935 generated, 0 forwarded
  Drop:  1 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
        0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 0 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
```

```
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 36 total, 0 forwarded broadcasts

TCP statistics:
  Rcvd: 654 total, 0 checksum errors, 0 no port
  Sent: 603 total

BGP statistics:
  Rcvd: 288 total, 8 opens, 0 notifications, 0 updates
        280 keepalives, 0 route-refresh, 0 unrecognized
  Sent: 288 total, 8 opens, 0 notifications, 0 updates
        280 keepalives, 0 route-refresh

OSPF statistics:
  Rcvd: 0 total, 0 checksum errors
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

  Sent: 0 total
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

IP-EIGRP statistics:
  Rcvd: 2303 total
  Sent: 2301 total

PIMv2 statistics: Sent/Received
  Total: 0/0, 0 checksum errors, 0 format errors
  Registers: 0/0 (0 non-rp, 0 non-sm-group), Register Stops: 0/0,  Hellos: 0/0
  Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
  Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0
  Queue drops: 0
  State-Refresh: 0/0

IGMP statistics: Sent/Received
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
  DVMRP: 0/0, PIM: 0/0
  Queue drops: 0

ARP statistics:
  Rcvd: 2 requests, 5 replies, 0 reverse, 0 other
  Sent: 1 requests, 3 replies (0 proxy), 0 reverse
```

Table 25 describes the significant fields shown in the display.

Table 25 show ip traffic Field Descriptions

Field	Description
IP statistics	Heading for IP statistics fields.
Total	Total number of packets.
Rcvd	Total received, and total destined for this device.
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
checksum errors	Indicates that the packet has a bad checksum value in the header.
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.

Table 25 show ip traffic Field Descriptions (continued)

Field	Description
unknown protocol	Indicates that the packet contains an unknown protocol value or type.
not a gateway	Non-routed packet.
security failures	Packets that with incorrect security values in the IP packet header.
bad options	Packets with incorrect options in the IP packet header.
with options	Packets with options configured in the IP packet header.
Opts	Field for IP packet options.
Frags	Field for packet fragmentation statistics.
Bcast	Field for broadcast packet statistics.
Mcast	Field for multicast packet statistics.
Sent	Field for transmitted packet statistics.
Drop	Field for dropped packet statistics.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram it did not know how to route.
ICMP statistics	Heading for ICMP statistics.
UDP statistics	Field for UDP packet statistics.
TCP	Field for TCP packet statistics.
BGP	Field for BGP packet statistics.
OSPF	Field for OSPF packet statistics.
IP-EIGRP	Field for EIGRP packet statistics.
PIMv2	Field for PIM statistics.
IGMP	Field for IGMP statistics.
ARP	Field for ARP statistics.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or who do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the command was made clearer and easier to understand.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

The following is sample output from the **show standby** command:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   120    Init     10.0.0.1        unknown         10.0.0.12
```

Table 26 describes the significant fields shown in the displays.

Table 26 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show "unknown." The state is listed as disabled in the fields when the **standby ip** command has not been specified.
Virtual IP address is, secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be "default," "bia," (burned-in address) or "confgd" (configured).
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in ...	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time a group will wait to synchronize with the IP redundancy clients.

Table 26 show standby Field Descriptions (continued)

Field	Description
Active router is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the "standby" router (the router that is next in line to be the Hot Standby router).
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the **standby track** command.
IP redundancy name is	The name of the HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show standby capability

To display the limitation on how many virtual MAC addresses that some interfaces can listen to, use the **show standby capability** command in user EXEC or privileged EXEC mode.

show standby capability [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

HSRP allows up to 256 groups to be configured on each interface, but it is possible that the MAC address filter of the interface does not support that many entries. For example, Versatile Interface Processor (VIP) interfaces only support 32 MAC addresses in their MAC address filter. If more HSRP groups are created than there are address filter entries, then it is likely that the router will stop listening to packets sent to the MAC address of an active HSRP group.

Examples

The following is sample output from the **show standby capability** command:

```
Router# show standby capability
7206VXR * indicates hardware may support HSRP
                                                  |
Interface          Type                          H  Potential Max Groups
FastEthernet0/0    18  DEC21140A                 *  256  (0x60194B00,
0x60194BE8)
FastEthernet1/0    18  DEC21140A                 *  256  (0x60194B00,
0x60194BE8)
Ethernet2/0        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/1        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/2        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/3        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/4        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/5        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/6        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/7        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
ATM3/0             74  ENHANCED ATM PA           *  256  LAN emulation
TokenRing4/0       66  HAWKEYE                   *  3    HSRP TR functional
```

```
addresses (0x6076A590)
TokenRing4/1       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/2       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/3       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
Serial5/0          67  M4T                      -
Serial5/1          67  M4T                      -
Serial5/2          67  M4T                      -
Serial5/3          67  M4T                      -
FastEthernet6/0    18  DEC21140A             *  256  (0x60194B00,
0x60194BE8)
VoIP-Null0         102 VoIP-Null                -
```

Table 27 describes the significant fields in the display.

Table 27 show standby capability Field Descriptions

Field	Description
Interface	Interface type and number for the interface.
Type	Hardware type.
*	Indicates hardware may support HSRP.
Potential Max Groups	An estimate of the number of HSRP groups that a MAC address filter can process for an interface.

show standby delay

To display Hot Standby Router Protocol (HSRP) information about delay periods, use the **show standby delay** command in user EXEC or privileged EXEC mode.

show standby delay [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output from the **show standby delay** command:

```
Router# show standby delay

 Interface           Minimum Reload
 Ethernet0/3         1       5
```

Related Commands

Command	Description
standby delay minimum reload	Delays the initialization of HSRP groups.

show standby internal

To display internal flags and conditions, use the **show standby internal** command in user EXEC or privileged EXEC mode.

show standby internal [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

This example shows a configuration example and the output from the **show standby internal** command for the configuration:

```
interface Ethernet2/0
 ip address 10.0.0.254 255.255.0.0
 standby use-bia
 standby version 2
 standby 1 ip 10.0.0.1
 standby 1 timers 2 6
 standby 1 priority 110
 standby 1 preempt

Router# show standby internal

Global           Confg: 0000
Et2/0 If hw      AmdP2, State 0x210040
Et2/0 If hw      Confg: 0001, USEBIA
Et2/0 If hw      Flags: 0000
Et2/0 If sw      Confg: 0040, VERSION
Et2/0 If sw      Flags: 0001, USEBIA
Et2/0 Grp 1      Confg: 0072, IP_PRI, PRIORITY, PREEMPT, TIMERS
Et2/0 Grp 1      Flags: 0000
```

The above output shows internal flags and hardware and software information for Ethernet interface 2/0. The output shows that HSRP group 1 is configured for priority, preemption, and the **standby timers** and **standby-use bia** commands have been configured.

Related Commands

Command	Description
show standby	Displays HSRP information.

show standby redirect

To display Internet Control Message Protocol (ICMP) redirect information on interfaces configured with the Hot Standby Router Protocol (HSRP), use the **show standby redirect** command in user EXEC or privileged EXEC mode.

show standby redirect [*ip-address* | *interface-type interface-number* [**active** | **passive** | **timers**]]

Syntax Description

ip-address	(Optional) Router IP address.
interface-type interface-number	(Optional) Interface type and number for which output is displayed.
active	(Optional) Active HSRP routers on the subnet.
passive	(Optional) Passive HSRP routers on the subnet.
timers	(Optional) HSRP ICMP redirect timers.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output from the **show standby redirect** command with no optional keywords:

```
Router# show standby redirect

Interface          Redirects Unknown   Adv      Holddown
Ethernet0/2        enabled   enabled   30       180
Ethernet0/3        enabled   disabled  30       180

Active          Hits   Interface          Group Virtual IP      Virtual MAC
10.19.0.7       0      Ethernet0/2        3     10.19.0.13      0000.0c07.ac03
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02

Passive         Hits   Interface          Expires in
10.19.0.6       0      Ethernet0/2        151.800
```

Table 28 describes the significant fields in the display.

Table 28 show standby redirect Field Descriptions

Field	Description
Interface	Interface type and number for the interface.
Redirects	Indicates whether redirects are enabled or disabled on the interface.
Unknown	Indicates whether redirects to an unknown router are enabled or disabled on the interface.
Adv	Number indicating the passive router advertisement interval in seconds.
Holddown	Number indicating the passive router hold interval in seconds.
Active	Active HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the active router.
Group	Hot standby group number.
Virtual IP	Virtual IP address of the active HSRP router.
Virtual MAC	Virtual MAC address of the active HSRP router.
Passive	Passive HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the passive router.
Expires in	Time in seconds for a virtual IP to expire and the holddown time to apply for filtering routes to the standby router.

The following is sample output from the **show standby redirect** command with a specific interface Ethernet 0/3:

```
Router# show standby redirect e0/3

Interface          Redirects Unknown   Adv      Holddown
Ethernet0/3        enabled   disabled  30       180

Active          Hits   Interface          Group Virtual IP      Virtual MAC
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02
```

The following is sample output from the **show standby redirect** command showing all active routers on interface Ethernet 0/3:

```
Router# show standby redirect e0/3 active

Active          Hits   Interface          Group Virtual IP      Virtual MAC
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02
```

The following is sample output from the **show standby redirect** *ip-address* command, where the IP address is the real IP address of the router:

```
Router# show standby redirect 10.19.0.7

Active          Hits   Interface          Group Virtual IP      Virtual MAC
10.19.0.7       0      Ethernet0/2        3     10.19.0.13      0000.0c07.ac03
```

Related Commands

Command	Description
show standby	Displays the HSRP information.
standby redirect	Enables ICMP redirect messages to be sent when HSRP is configured on an interface.

show tcp statistics

To display TCP statistics, use the **show tcp statistics** EXEC command.

show tcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following is sample output from the **show tcp statistics** command:

```
Router# show tcp statistics

Rcvd: 210 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      132 packets (26640 bytes) in sequence
      5 dup packets (502 bytes)
      0 partially dup packets (0 bytes)
      0 out-of-order packets (0 bytes)
      0 packets (0 bytes) with data after window
      0 packets after close
      0 window probe packets, 0 window update packets
      0 dup ack packets, 0 ack packets with unsend data
      69 ack packets (3044 bytes)
Sent: 175 Total, 0 urgent packets
      16 control packets (including 1 retransmitted)
      69 data packets (3029 bytes)
      0 data packets (0 bytes) retransmitted
      73 ack only packets (49 delayed)
      0 window probe packets, 17 window update packets
7 Connections initiated, 1 connections accepted, 8 connections established
8 Connections closed (including 0 dropped, 0 embryonic dropped)
1 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

Table 29 describes the significant fields shown in the display.

Table 29 show tcp statistics Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
Total	Total number of TCP packets received.
no port	Number of packets received with no port.
checksum error	Number of packets received with checksum error.
bad offset	Number of packets received with bad offset to data.

Table 29 show tcp statistics Field Descriptions (continued)

Field	Description
too short	Number of packets received that were too short.
packets in sequence	Number of data packets received in sequence.
dup packets	Number of duplicate packets received.
partially dup packets	Number of packets received with partially duplicated data.
out-of-order packets	Number of packets received out of order.
packets with data after window	Number of packets received with data that exceeded the window size of the receiver.
packets after close	Number of packets received after the connection was closed.
window probe packets	Number of window probe packets received.
window update packets	Number of window update packets received.
dup ack packets	Number of duplicate acknowledgment packets received.
ack packets with unsend data	Number of acknowledgment packets received with unsent data.
ack packets	Number of acknowledgment packets received.
Sent:	Statistics in this section refer to packets sent by the router.
Total	Total number of TCP packets sent.
urgent packets	Number of urgent packets sent.
control packets	Number of control packets (SYN, FIN, or RST) sent.
data packets	Number of data packets sent.
data packets retransmitted	Number of data packets re-sent.
ack only packets	Number of packets sent that are acknowledgments only.
window probe packets	Number of window probe packets sent.
window update packets	Number of window update packets sent.
Connections initiated	Number of connections initiated.
connections accepted	Number of connections accepted.
connections established	Number of connections established.
Connections closed	Number of connections closed.
Total rxmt timeout	Number of times the router tried to resend, but timed out.
connections dropped in rxmit timeout	Number of connections dropped in the resend timeout.
Keepalive timeout	Number of keepalive packets in the timeout.
keepalive probe	Number of keepalive probes.
Connections dropped in keepalive	Number of connections dropped in the keepalive.

Related Commands

Command	Description
clear tcp statistics	Clears TCP statistics.

standby authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **standby authentication** interface configuration command. To delete an authentication string, use the **no** form of this command.

standby [*group-number*] **authentication** [**mode text**] *string*

no standby [*group-number*] **authentication** [**mode text**] *string*

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies.
mode text	(Optional) Indicates use of a plain text authentication mode.
string	Authentication string. It can be up to eight characters long. The default string is **cisco**.

Defaults

The default group number is 0. The default string is **cisco**.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **mode** and **text** keywords were added.

Usage Guidelines

HSRP ignores unauthenticated HSRP messages.

The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

The following example configures “company1” as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
interface ethernet 0
 standby 1 authentication mode text company1
```

standby delay minimum reload

To configure the delay period before the initialization of Hot Standby Router Protocol (HSRP) groups, use the **standby delay minimum reload** interface configuration command. To disable the delay period, use the **no** form of this command.

standby delay minimum *min-delay* **reload** *reload-delay*

no standby delay minimum *min-delay* **reload** *reload-delay*

Syntax Description

min-delay	Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events.
reload-delay	Time (in seconds) to delay after the router has reloaded. This delay period only applies to the first interface-up event after the router has reloaded.

Defaults

The default minimum delay is 1 second.

The default reload delay is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

If the active router fails or is removed from the network, then the standby router will automatically become the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, in some cases, even if the **standby preempt** command is not configured, the former active router will resume the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay period for HSRP group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through and it is not necessary to configure longer delay values.

The delay will be cancelled if an HSRP packet is received on an interface.

You can view the delays with the **show standby delay** command.

Examples

The following example sets the minimum delay period to 30 seconds and the delay period after the first reload to 120 seconds:

```
interface ethernet 0
```

```
ip address 10.20.0.7 255.255.0.0
standby delay minimum 30 reload 120
standby 3 ip 10.20.0.21
standby 3 timers msec 300 msec 700
standby 3 priority 100
```

Related Commands

Command	Description
show standby delay	Displays HSRP information about delay periods.
standby preempt	Configures the HSRP preemption and preemption delay.
standby timers	Configures the time between hello packets and the time before other routers declare the active HSRP or standby router to be down.

standby ip

To activate the Hot Standby Router Protocol (HSRP), use the **standby ip** interface configuration command. To disable HSRP, use the **no** form of this command.

standby [*group-number*] **ip** [*ip-address* [**secondary**]]

no standby [*group-number*] **ip** [*ip-address*]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
ip-address	(Optional) IP address of the Hot Standby router interface.
secondary	(Optional) Indicates the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

Defaults

The default group number is 0.

HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *group-number* argument was added.
11.1	The **secondary** keyword was added.

Usage Guidelines

The **standby ip** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the designated address is learned through the standby function. For HSRP to elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When the **standby ip** command is enabled on an interface, the handling of proxy ARP requests is changed (unless proxy ARP was disabled). If the Hot Standby state of the interface is active, proxy ARP requests are answered using the MAC address of the Hot Standby group. If the interface is in a different state, proxy ARP responses are suppressed.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

The following example activates HSRP for group 1 on Ethernet interface 0. The IP address used by the Hot Standby group will be learned using HSRP.

```
interface ethernet 0
 standby 1 ip
```

In the following example, all three virtual IP addresses appear in the ARP table using the same (single) virtual MAC address. All three virtual IP addresses are using the same HSRP group (group 0).

```
ip address 1.1.1.1. 255.255.255.0
ip address 1.2.2.2. 255.255.255.0 secondary
ip address 1.3.3.3. 255.255.255.0 secondary
ip address 1.4.4.4. 255.255.255.0 secondary
standby ip 1.1.1.254
standby ip 1.2.2.254 secondary
standby ip 1.3.3.254 secondary
```

standby mac-address

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **standby mac-address** interface configuration command. To revert to the standard virtual MAC address (0000.0C07.AC*xy*), use the **no** form of this command.

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
mac-address	MAC address.

Defaults

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command cannot be used on a Token Ring interface.

HSRP is used to help end stations locate the first hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, it is often necessary to be able to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **standby mac-address** command to specify the virtual MAC address.

The MAC address specified is used as the virtual MAC address when the router is active.

This command is intended for certain APPN configurations. The parallel terms are shown in Table 30.

Table 30 Parallel Terms Between APPN and IP

APPN	IP
End node	Host
Network node	Router or gateway

In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **standby mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes.

Examples

If the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node, the following example shows the command used to configure HSRP group 1 with the virtual MAC address:

```
standby 1 mac-address 4000.1000.1060
```

Related Commands

Command	Description
show standby	Displays HSRP information.
standby use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address.

standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when the Hot Standby Router Protocol (HSRP) is running over FDDI, use the **standby mac-refresh** interface configuration command. To restore the default value, use the **no** form of this command.

standby mac-refresh *seconds*

no standby mac-refresh

Syntax Description

seconds	Number of seconds in the interval at which a packet is sent to refresh the MAC cache. The maximum value is 255 seconds. The default is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command applies to HSRP running over FDDI only. Packets are sent every 10 seconds to refresh the MAC cache on learning bridges or switches. By default, the MAC cache entries age out in 300 seconds (5 minutes).

All other routers participating in HSRP on the FDDI ring receive the refresh packets, although the packets are intended only for the learning bridge or switch. Use this command to change the interval. Set the interval to 0 if you want to prevent refresh packets (if you have FDDI but do not have a learning bridge or switch).

Examples

The following example changes the MAC refresh interval to 100 seconds. Therefore, a learning bridge would need to miss three packets before the entry ages out.

```
standby mac-refresh 100
```

standby name

To configure the name of the standby group, use the **standby name** command in interface configuration mode. To disable the name, use the **no** form of this command.

standby name *group-name*

no standby name *group-name*

Syntax Description

group-name	Specifies the name of the standby group.

Defaults

The Hot Standby Router Protocol (HSRP) is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The name specifies the HSRP group used. The HSRP group name must be unique on the router.

Examples

The following example specifies the standby name as SanJoseHA:

```
interface ethernet0
 ip address 10.0.0.1 255.0.0.0
 standby ip 10.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110
```

Related Commands

Command	Description
ip mobile home-agent redundancy	Configures the home agent for redundancy.

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **preempt** [**delay**{**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

no standby [*group-number*] **preempt** [**delay**{**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *seconds*	(Optional) Specifies the minimum delay period in seconds. The *seconds* argument causes the local router to postpone taking over the active role for a minimum number of seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *seconds*	(Optional) Specifies the preemption delay, in seconds, after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
sync *seconds*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in seconds.

Defaults

The default group number is 0.
The default delay is 0 seconds; if the router wants to preempt, it will do so immediately.
By default, the router that comes up later becomes the standby.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.2	The **reload** keyword was added.
12.4(4)T	Support for IPv6 was added.
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.

Usage Guidelines

When this command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If preemption is not configured, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it will become the active router, yet it is unable to provide adequate routing services. Solve this problem by configuring a delay before the preempting router actually preempts the currently active router.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

IP redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *seconds* command specifies a maximum number of seconds to allow IP redundancy clients to prevent preemption. When this expires, then preemption takes place regardless of the state of the IP redundancy clients.

The **standby preempt delay reload** *seconds* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command will disable the preemption delay but preemption will remain enabled. The **no standby preempt delay minimum** *seconds* command will disable the minimum delay but leave any synchronization delay if it was configured.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router will wait for 300 seconds (5 minutes) before attempting to become the active router:

```
interface ethernet 0
 standby ip 172.19.108.254
 standby preempt delay minimum 300
```

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. The default group number is 0.
priority	Priority value that prioritizes a potential Hot Standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.

Defaults

The default group number is 0.
The default priority is 100.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.4(4)T	Support for IPv6 was added.
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.

Usage Guidelines

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

Note that the priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router has a priority of 120 (higher than the default value):

```
interface ethernet 0
 standby ip 172.19.108.254
 standby priority 120
 standby preempt delay 300
```

Related Commands

Command	Description
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

standby redirect

To enable Hot Standby Router Protocol (HSRP) filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirects** command in interface configuration mode. To disable the HSRP filtering of ICMP redirect messages, use the **no** form of this command.

standby redirect [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

no standby redirects [**unknown**]

Syntax Description

enable	(Optional) Allows the filtering of ICMP redirect messages on interfaces configured with HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.
disable	(Optional) Disables the filtering of ICMP redirect messages on interfaces configured with HSRP.
timers	(Optional) Adjusts HSRP router advertisement timers.
advertisement	(Optional) HSRP Router advertisement interval in seconds. This is an integer from 10 to 180. The default is 60 seconds.
holddown	(Optional) HSRP router holddown interval in seconds. This is an integer from 61 to 3600. The default is 180 seconds.
unknown	(Optional) Allows sending of ICMP packets when the next hop IP address contained in the packet is unknown in the HSRP table of real IP addresses and active virtual IP addresses. The **no standby redirect unknown** command stops the redirects from being sent.

Defaults

HSRP filtering of ICMP redirect messages is enabled if HSRP is configured on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	The following keywords and arguments were added to the command: • **timers** *advertisement holdtime* • **unknown**

Usage Guidelines

The **standby redirect** command can be configured globally or on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface will inherit the global value. If the filtering of ICMP redirects is explicitly disabled on an interface, then the global command cannot reenable this functionality.

The **no standby redirect** command is the same as the **standby redirect disable** command. However, it is not desirable to save the **no** form of this command to NVRAM. Because the command is enabled by default, it is preferable to use the **standby redirect disable** command to disable the functionality.

With the **standby redirect** command enabled, the real IP address of a router can be replaced with a virtual IP address in the next hop address or gateway field of the redirect packet. HSRP looks up the next hop IP address in its table of real IP addresses versus virtual IP addresses. If HSRP does not find a match, the HSRP router allows the redirect packet to go out unchanged. The host HSRP router is redirected to a router that is unknown, that is, a router with no active HSRP groups. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

Examples

The following example allows HSRP to filter ICMP redirect messages on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirect
Router(config-if)# standby 1 ip 10.0.0.11
```

The following example shows how to change the HSRP router advertisement interval to 90 seconds and the holddown timer to 270 seconds on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirect timers 90 270
Router(config-if)# standby 1 ip 10.0.0.11
```

Related Commands

Command	Description
show standby	Displays the HSRP information.
show standby redirect	Displays ICMP redirect information on interfaces configured with the HSRP.

standby timers

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **standby timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply. The default is 0.
msec	(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
hellotime	Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, hello interval is in milliseconds. This is an integer from 15 to 999.
holdtime	Time (in seconds) before the active or standby router is declared to be down. This is an integer from *x* to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from *y* to 3000. Where: • *x* is the *hellotime* + 50 milliseconds, then rounded up to the nearest 1 second • *y* is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

Defaults

The default group number is 0.
The default hello interval is 3 seconds.
The default hold time is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **msec** keyword was added.
12.2	The minimum values of *hellotime* and *holdtime* in milliseconds changed.
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.

Usage Guidelines

The **standby timers** command configures the time between standby hello packets and the time before other routers declare the active or standby router to be down. Routers or access servers on which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, holdtime is greater than or equal to 3 times the value of hellotime. The range of values for holdtime force the holdtime to be greater than the hellotime. If the timer values are specified in milliseconds, the holdtime is required to be at least three times the hellotime value and not less than 50 milliseconds.

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used on Cisco 7200 platforms or better, and on Fast-Ethernet or FDDI interfaces or better. Setting the **process-max-time** command to a suitable value may also help with flapping.

The value of the standby timer will not be learned through HSRP hellos if it is less than 1 second.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.
```

Examples

The following example sets, for group number 1 on Ethernet interface 0, the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds:

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

The following example sets, for the Hot Router interface located at 172.19.10.1 on Ethernet interface 0, the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds:

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

The following example sets, for the Hot Router interface located at 172.18.10.1 on Ethernet interface 0, the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds. Note that the holdtime is larger than three times the hellotime because the minimum holdtime value in milliseconds is 50.

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

standby track

To configure an interface so that the Hot Standby priority changes based on the availability of other interfaces, use the **standby track** interface configuration command. To remove the tracking, use the **no** form of this command.

standby [*group-number*] **track** *interface-type interface-number* [*interface-priority*]

no standby [*group-number*] **track** *interface-type interface-number* [*interface-priority*]

Syntax Description

group-number	(Optional) Group number on the interface to which the tracking applies.
interface-type	Interface type (combined with interface number) that will be tracked.
interface-number	Interface number (combined with interface type) that will be tracked.
interface-priority	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.

Defaults

The default group number is 0.

The default interface priority is 10.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command ties the Hot Standby priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for the Hot Standby Router Protocol (HSRP).

When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

The optional *interface-priority* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount.

When multiple tracked interfaces are down, the decrements are cumulative whether configured with *interface-priority* values or not.

A tracked interface is considered down if the IP address is disabled on that interface.

If HSRP is configured to track an interface, and that interface is physically removed as in the case of an online insertion and removal (OIR) operation, then HSRP will regard the interface as always down. Further, it will not be possible to remove the HSRP interface tracking configuration. To prevent this problem, use the **no standby track** i*nterface-type interface-number* command before you physically remove the interface.

Use the **no standby** *group-number* **track** command to delete all tracking configuration for a group.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

In the following example, Ethernet interface 1 tracks Ethernet interface 0 and serial interface 0. If one or both of these two interfaces go down, the Hot Standby priority of the router decreases by 10. Because the default Hot Standby priority is 100, the priority becomes 90 when one or both of the tracked interfaces go down.

```
interface ethernet 1
 ip address 198.92.72.37 255.255.255.240
 no ip redirects
 standby track ethernet 0
 standby track serial 0
 standby preempt
 standby ip 198.92.72.46
```

Related Commands

Command	Description
show standby	Displays HSRP information.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.

standby use-bia

To configure the Hot Standby Router Protocol (HSRP) to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** interface configuration command. To restore the default virtual MAC address, use the **no** form of this command.

standby use-bia [**scope interface**]

no standby use-bia

Syntax Description

scope interface	(Optional) Specifies that this command is configured just for the subinterface on which it was entered, instead of the major interface.

Defaults

HSRP uses the preassigned MAC address on Ethernet and FDDI, or the functional address on Token Ring.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1	The behavior was modified to allow multiple standby groups to be configured for an interface configured with this command

Usage Guidelines

For an interface with this command configured, multiple standby group can be configured. Hosts on the interface must have a default gateway configured. We recommend that you set the **no ip proxy-arp** command on the interface. It is desirable to configure the **standby use-bia** command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses set to a functional address.

When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

Without the **scope interface** keywords, the **standby use-bia** command applies to all subinterfaces on the major interface. The **standby use-bia** command may not be configured both with and without the **scope interface** keywords at the same time.

Examples

In the following example, the burned-in address of Token Ring interface 4/0 will be the virtual MAC address mapped to the virtual IP address:

```
interface token4/0
 standby use-bia
```

start-forwarding-agent

To start the Forwarding Agent, use the **start-forwarding-agent** CASA-port configuration command.

start-forwarding-agent *port-number* [*password* [*timeout*]]

Syntax Description

port-number	Port numbers on which the Forwarding Agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
password	(Optional) Text password used for generating the MD5 digest.
timeout	(Optional) Duration (in seconds) during which the Forwarding Agent will accept the new and old password. Valid range is from 0 to 3600 seconds. The default is 180 seconds.

Defaults

The default initial number of affinities is 5000.

The default maximum number of affinities is 30,000.

Command Modes

CASA-port configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The Forwarding Agent must be started before you can configure any port information for the forwarding agent.

Examples

The following example specifies that the forwarding agent will listen for wildcard and fixed affinities on port 1637:

```
start-forwarding-agent 1637
```

Related Commands

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

transmit-interface

To assign a transmit interface to a receive-only interface, use the **transmit-interface** interface configuration command. To return to normal duplex Ethernet interfaces, use the **no** form of this command.

transmit-interface *type number*

no transmit-interface

Syntax Description

type	Transmit interface type to be linked with the (current) receive-only interface.
number	Transmit interface number to be linked with the (current) receive-only interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Receive-only interfaces are used commonly with microwave Ethernet links.

Examples

The following example specifies Ethernet interface 0 as a simplex Ethernet interface:

```
interface ethernet 1
 ip address 128.9.1.2
 transmit-interface ethernet 0
```