



IP Services Commands

Use the commands in this chapter to configure various IP services. For configuration information and examples on IP services, refer to the “Configuring IP Services” chapter of the *Network Protocols Configuration Guide, Part 1*.

access-class

To restrict incoming and outgoing connections between a particular virtual terminal line (into a Cisco device) and the addresses in an access list, use the **access-class** line configuration command. To remove access restrictions, use the **no** form of this command.

```
access-class access-list-number {in | out}  
no access-class access-list-number {in | out}
```

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 199.
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Default

No access lists are defined.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Remember to set *identical restrictions* on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line EXEC** command and specify the line number.

Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0 0.0.0.255  
line 1 5  
access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 36.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 36.0.0.0 0.255.255.255  
line 1 5  
access-class 10 out
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show line

access-list (extended)

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, use the **no** form of this command.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    protocol source source-wildcard destination destination-wildcard [precedence precedence]
    [tos tos] [log | log-input]
no access-list access-list-number
```

For Internet Control Message Protocol (ICMP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    icmp source source-wildcard destination destination-wildcard [icmp-type | [[icmp-type
    icmp-code] | [icmp-message]]] [precedence precedence] [tos tos] [log | log-input]
```

For Internet Group Management Protocol (IGMP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    igmp source source-wildcard destination destination-wildcard [igmp-type]
    [precedence precedence] [tos tos] [log | log-input]
```

For TCP, you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    tcp source source-wildcard [operator port [port]] destination destination-wildcard
    [operator port [port]] [established] [precedence precedence] [tos tos] [log | log-input]
```

For User Datagram Protocol (UDP), you can also use the following syntax:

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
    udp source source-wildcard [operator port [port]] destination destination-wildcard
    [operator port [port]] [precedence precedence] [tos tos] [log | log-input]
```



Caution Enhancements to this command are backward compatible; migrating from releases prior to Release 11.1 will convert your access lists automatically. However, releases prior to Release 11.1 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 11.1, the resulting access list will not be interpreted correctly. **This could cause you severe security problems.** Save your old configuration file before booting these images.

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 100 to 199.
dynamic <i>dynamic-name</i>	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Traffic Filters” chapter in the <i>Security Configuration Guide</i> .
timeout <i>minutes</i>	(Optional) Specifies the absolute length of time (in minutes) that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Traffic Filters” chapter in the <i>Security Configuration Guide</i> .
deny	Denies access if the conditions are matched.

permit	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an IP 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 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the keyword ip . Some protocols allow further qualifiers described below.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to the source. Each wildcard bit set to zero indicates that the corresponding bit position in the packet's ip address must exactly match the bit value in the corresponding bit position in the source. Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's ip address will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. For example, 0.0.255.255 to require an exact match of only the first 16 bits of the <i>source</i>.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. Wildcard bits set to one do not need to be contiguous in the <i>source-wildcard</i> . For example, a <i>source-wildcard</i> of 0.255.0.64 would be valid.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	<p>(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.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the section “Usage Guidelines.”</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(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.</p>
<i>icmp-message</i>	<p>(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.”</p>
<i>igmp-type</i>	<p>(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.”</p>
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	<p>(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names are listed in the section “Usage Guidelines.” TCP port names can only be used when filtering TCP. UDP port names are listed in the section “Usage Guidelines.” UDP port names can only be used when filtering UDP.</p> <p>TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.</p>

- 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.
- 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.
- 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.
- log-input** (Optional) Includes the input interface and source MAC address or VC in the logging output.

Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Mode

Global configuration

Usage Guidelines

The UDP form of this command first appeared in Cisco IOS Release 10.0. All other forms of the command, as well as the following arguments and keywords, first appeared in Cisco IOS Release 10.3:

source
source-wildcard
destination
destination-wildcard
precedence *precedence*
icmp-type
icm-code
icmp-message
igmp-type

operator
port
established

The following keywords and arguments first appeared in Cisco IOS Release 11.1:

dynamic *dynamic-name*
timeout *minutes*

The following keyword first appeared in Cisco IOS Release 11.2:

log-input

You can use access lists to control the transmission of packets on an interface, control virtual terminal line access, and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match against the TCP source port, the type of service value, or the packet's precedence.

Note After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of type of service (TOS) names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**

- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**

- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found by typing a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**

- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found by typing a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Examples

In the following example, serial interface 0 is part of a Class B network with the address 128.88.0.0, and the mail host's address is 128.88.1.2. The keyword **established** is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicate that the packet belongs to an existing connection.

access-list (extended)

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example also permit Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. They are similar to the bitmasks that are used with normal access lists. Prefix/mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix/mask bits corresponding to wildcard bits set to 0 are used in comparison.

In the following example, permit 192.108.0.0 255.255.0.0 but deny any more specific routes of 192.108.0.0 (including 192.108.0.0 255.255.255.0).

```
access-list 101 permit ip 192.108.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

In the following example, permit 131.108.0/24 but deny 131.108/16 and all other subnets of 131.108.0.0.

```
access-list 101 permit ip 131.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-class

access-list (standard)

clear access-temp

distribute-list in

distribute-list out

ip access-group

ip access-list

logging console

priority-list

queue-list

show access-lists

show ip access-list

access-list (standard)

To define a standard IP access list, use the standard version of the **access-list** global configuration command. To remove a standard access lists, use the **no** form of this command.

```
access-list access-list-number {deny | permit} source [source-wildcard]  
no access-list access-list-number
```



Caution Enhancements to this command are backward compatible; migrating from releases prior to Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This could cause you severe security problems.** Save your old configuration file before booting these images.

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 99.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>source</i>	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the source. Each wildcard bit set to zero indicates that the corresponding bit position in the packet's ip address must exactly match the bit value in the corresponding bit position in the source. Each wildcard bit set to one indicates that both a zero bit and a one bit in the corresponding position of the packet's ip address will be considered a match to this access list entry. There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. For example, 0.0.255.255 to require an exact match of only the first 16 bits of the <i>source</i>.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. Wildcard bits set to one do not need to be contiguous in the <i>source-wildcard</i> . For example, a <i>source-wildcard</i> of 0.255.0.64 would be valid.

Default

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control virtual terminal line access, and restrict the contents of routing updates.

Use the **show access-lists EXEC** command to display the contents of all access lists.

Use the **show ip access-list EXEC** command to display the contents of one access list.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0 0.0.0.255
access-list 1 permit 128.88.0.0 0.0.255.255
access-list 1 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-class

access-list (extended)

distribute-list in

distribute-list out

ip access-group

priority-list

queue-list

show access-lists

show ip access-list

clear access-list counters

To clear the counters of an access list, use the **clear access-list counters** EXEC command.

clear access-list counters {*access-list-number* | *name*}

Syntax Description

<i>access-list-number</i>	Access list number from 0 to 1199 for which to clear the counters.
<i>name</i>	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Some access lists keep counters that count the number of packets that pass each line of an access list. The **show access-lists** command displays the counters as a number of matches. Use the **clear access-list counters** command to restart the counters for a particular access list to 0.

Example

The following example clears the counters for access list 101:

```
clear access-list counters 101
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show access-lists

clear ip accounting

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

clear ip accounting [checkpoint]

Syntax Description

checkpoint (Optional) Clears the checkpointed database.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You can also clear the checkpointed database by issuing the **clear ip accounting** command twice in succession.

Example

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

```
clear ip accounting
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip accounting
ip accounting-list
ip accounting-threshold
ip accounting-transits
show ip accounting

clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** EXEC command.

```
clear ip drp
```

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Example

The following example clears all DRP statistics:

```
clear ip drp
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip drp access-group

ip drp authentication key-chain

clear tcp statistics

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

clear tcp statistics

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example clears all TCP statistics:

```
clear tcp statistics
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show tcp statistics

deny

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

deny *source* [*source-wildcard*]

no deny *source* [*source-wildcard*]

deny *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]

no deny *protocol source source-wildcard destination destination-wildcard*

For ICMP, you can also use the following syntax:

deny icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For IGMP, you can also use the following syntax:

deny igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For TCP, you can also use the following syntax:

deny tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For UDP, you can also use the following syntax:

deny udp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**]

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP 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 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.• Use the keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	<p>(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.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</p>

<i>icmp-message</i>	(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 “Usage Guidelines” section of the access-list (extended) command.
<i>igmp-type</i>	(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 “Usage Guidelines” section of the access-list (extended) command.
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	(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 “Usage Guidelines” section of the access-list (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.
log	<p>(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.)</p> <p>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.</p> <p>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.</p>

Default

There is no specific condition under which a packet is denied passing the named access list.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

Example

The following example sets a deny condition 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)
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip access-group

ip access-list

permit

show ip access-list

dynamic

To define a named, dynamic, IP access list, use the **dynamic** access-list configuration command. To remove the access lists, use the **no** form of this command.

```
dynamic dynamic-name [timeout minutes] {deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence] [tos tos] [log]
no dynamic dynamic-name
```

For ICMP, you can also use the following syntax:

```
dynamic dynamic-name [timeout minutes] {deny | permit} icmp source source-wildcard
destination destination-wildcard [icmp-type [icmp-code] | icmp-message] [precedence
precedence] [tos tos] [log]
```

For IGMP, you can also use the following syntax:

```
dynamic dynamic-name [timeout minutes] {deny | permit} igmp source source-wildcard
destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log]
```

For TCP, you can also use the following syntax:

```
dynamic dynamic-name [timeout minutes] {deny | permit} tcp source source-wildcard
[operator port [port]] destination destination-wildcard [operator port [port]] [established]
[precedence precedence] [tos tos] [log]
```

For UDP, you can also use the following syntax:

```
dynamic dynamic-name [timeout minutes] {deny | permit} udp source source-wildcard
[operator port [port]] destination destination-wildcard [operator port [port]] [precedence
precedence] [tos tos] [log]
```



Caution Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Syntax Description

<i>dynamic-name</i>	Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Traffic Filters” chapter in the <i>Security Configuration Guide</i> .
timeout <i>minutes</i>	(Optional) Specifies the absolute length of time (in minutes) that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Traffic Filters” chapter in the <i>Security Configuration Guide</i> .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an IP 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 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.• Use the keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	<p>(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.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the section “Usage Guidelines.”</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</p>

<i>icmp-message</i>	(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.”
<i>igmp-type</i>	(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.”
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	(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 “Usage Guidelines” section of the access-list (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.
log	<p>(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.)</p> <p>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.</p> <p>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.</p>

Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match against the TCP source port, the type of service value, or the packet's precedence.

Note After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of type of service (TOS) names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**

- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**

- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found by typing a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**

- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found by typing a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Example

In the following example, the access list named washington is a dynamic access list.

```
ip access-group washington in
!
ip access-list extended washington
dynamic testlist timeout 5
permit ip any any
permit tcp any host 185.302.21.2 eq 23
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear access-temp
distribute-list in
distribute-list out
ip access-group
ip access-list
logging console
priority-list
queue-list
show access-lists
show ip access-list

ip access-group

To control access to an interface, use the **ip access-group** interface configuration command. To remove the specified access group, use the **no** form of this command.

```
ip access-group {access-list-number | name} {in | out}  
no ip access-group {access-list-number | name} {in | out}
```

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 199.
<i>name</i>	Name of an IP access list as specified by an ip access-list command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Default

Entering a keyword is strongly recommended, but if a keyword is not specified, **out** is the default.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The *name* argument first appeared in Cisco IOS Release 11.2.

Access lists are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP Host Unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software transmits the packet. If the access list rejects the address, the software discards the packet and returns an ICMP Host Unreachable message.

If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any cBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—an SSE configured with simple access lists can still switch packets, on output only).

Example

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
interface ethernet 0  
ip access-group 101 out
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)

access-list (standard)

ip access-list

show access-lists

ip access-list

To define an IP access list by name, use the **ip access-list** global configuration command. To remove a named IP access lists, use the **no** form of this command.

```
ip access-list {standard | extended} name  
no ip access-list {standard | extended} name
```



Caution Named access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Default

There is no named IP access list.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command to configure a named IP access list as opposed to a numbered IP access list. This command will take you into access-list configuration mode, where you must define the denied or permitted access conditions with the **deny** and **permit** commands.

Specifying **standard** or **extended** with the **ip access-list** command determines the prompt you get when you enter access-list configuration mode.

Use the **ip access-group** command to apply the access-list to an interface.

Named access lists are not compatible with Cisco IOS releases prior to Release 11.2.

Example

The following example defines a standard access list named Internetfilter:

```
ip access-list standard Internetfilter  
  permit 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)
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

deny

ip access-group

permit

show ip access-list

ip accounting

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

```
ip accounting [access-violations]  
no ip accounting [access-violations]
```

Syntax Description

access-violations (Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

IP accounting records the number of bytes (IP header and data) and packets switched through the system on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the router access server or terminating in this device is not included in the accounting statistics.

The **access-violations** option first appeared in IOS Release 10.3. If you specify the **access-violations** keyword, **ip accounting** provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data might also indicate that you should verify IP access list configurations. To receive a logging message on the console when an extended access list entry denies a packet access (to log violations), include the **log** keyword in the **access-list (extended)** command.

Statistics are accurate even if IP fast switching or IP access lists are being used on the interface.

IP accounting disables autonomous switching and SSE switching on the interface.

Example

The following example enables IP accounting on Ethernet interface 0:

```
interface ethernet 0  
  ip accounting
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)
clear ip accounting
ip accounting-list
ip accounting-threshold
ip accounting-transits
show ip accounting

ip accounting-list

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

```
ip accounting-list ip-address wildcard  
no ip accounting-list ip-address wildcard
```

Syntax Description

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

Default

No filters are defined.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The source and destination address of each IP datagram is logically ANDed with the wildcard bits and compared with the *ip-address*. If there is a match, the information about the IP datagram will be entered into the accounting database. If there is no match, the IP datagram is considered a *transit* datagram and will be counted according to the setting of the **ip accounting-transits** global configuration command.

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
clear ip accounting  
ip accounting  
ip accounting-threshold  
ip accounting-transits  
show ip accounting
```

ip accounting-threshold

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

```
ip accounting-threshold threshold  
no ip accounting-threshold threshold
```

Syntax Description

threshold Maximum number of entries (source and destination address pairs) that the Cisco IOS software accumulates.

Default

512 entries

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

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

Example

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

```
ip accounting-threshold 500
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
clear ip accounting  
ip accounting  
ip accounting-list  
ip accounting-transits  
show ip accounting
```


ip drp access-group

To control the sources of Director Response Protocol (DRP) queries to the DRP Server Agent, use the **ip drp access-group** global configuration command. To remove the access list, use the **no** form of this command.

```
ip drp access-group access-list-number  
no ip drp access-group access-list-number
```

Syntax Description

access-list-number Number of a standard IP access list in the range 1 to 99.

Default

The DRP Server Agent will answer all queries.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

This command applies an access list to the interface, thereby controlling who can send queries to the DRP Server Agent.

If both an authentication key chain and an access group have been specified, both security measures must permit access before a request is processed.

Example

The following example configures access list 1, which permits only queries from the host at 33.45.12.4:

```
access-list 1 permit 33.45.12.4  
ip drp access-group 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip drp authentication key-chain
show ip drp

ip drp authentication key-chain

To configure authentication on the DRP Server Agent for DistributedDirector, use the **ip drp authentication key-chain** global configuration command. To remove the key chain, use the **no** form of this command.

```
ip drp authentication key-chain name-of-chain  
no ip drp authentication key-chain name-of-chain
```

Syntax Description

name-of-chain Name of the key chain containing one or more authentication keys.

Default

No authentication is configured for the DRP Server Agent.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

When a key chain and key are configured, the key is used to authenticate all Director Response Protocol requests and responses. The active key on the DRP Server Agent must match the active key on the primary agent. Use the **key** and **key-string** commands to configure the key.

Example

The following example configures a key chain named *ddchain*:

```
ip drp authentication key-chain ddchain
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

accept-lifetime
ip drp access-group
key
key chain
key-string
send-lifetime
show ip drp
show key chain

ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** global configuration command. To disable the DRP Server Agent, use the **no** form of this command.

ip drp server
no ip drp server

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Example

The following example enables the DRP Server Agent:

```
ip drp server
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip drp access-group
ip drp authentication key-chain
show ip drp

ip mask-reply

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

ip mask-reply
no ip mask-reply

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

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

```
interface ethernet 0
 ip address 131.108.1.0 255.255.255.0
 ip mask-reply
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** 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.

Default

Minimum is 128 bytes; maximum depends on interface medium.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

Example

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

You can use the master indexes or search online to find documentation of related commands.

mtu

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.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

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

```
ip source-route
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ping (privileged)
ping (user)

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.

Default

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 9.1.

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

Example

The following example sets the maximum TCP read size to 64000 bytes:

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


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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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 Point-to-Point (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 while 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 means that fast interfaces like T1 can overload the router. Consider your network's traffic characteristics before using this command.

Example

In the following example, the first serial interface is set for header compression with a maximum of ten cache entries:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip tcp compression-connections

ip tcp path-mtu-discovery

To enable Path MTU Discovery for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** interface configuration command. To disable the feature, 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.

infinite (Optional) Turns off the age-timer.

Default

Disabled. If enabled, default *minutes* is 10 minutes.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3. The **age-timer** and **infinite** keywords first appeared in Cisco IOS Release 11.2.

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the end points 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. This might include customers using RSRB with TCP encapsulation, STUN, X.25 Remote Switching (also known as XOT, or X.25 over TCP), and some protocol translation configurations.

The age timer is a time interval for how often TCP re-estimates the Path MTU with a larger MSS. By using the age timer, TCP Path MTU becomes a dynamic process. If 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.

Example

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 there is no TTY associated with it, the default value is 20 segments.

Default

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

Example

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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

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 retransmit packets early, but such retransmitted segments might have already been successfully 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 retransmit only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when multiple 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.

Example

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

```
ip tcp selective-ack
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip 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.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

In previous versions of Cisco IOS software, 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 dial-up 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 see this problem.

Example

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 timestamp, use the **ip tcp timestamp** global configuration command. To disable TCP timestamp, use the **no** form of this command.

ip tcp timestamp
no ip tcp timestamp

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

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

This feature must be disabled if you want to use TCP header compression.

Example

The following example enables the router to send TCP timestamps:

```
ip tcp timestamp
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip 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 65535 bytes. The default value is 2144 bytes.

Default

2144 bytes

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 9.1.

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.

Example

The following example sets the TCP window size to 1000 bytes:

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

ip unreachable

To enable the generation of ICMP Unreachable messages, use the **ip unreachable** interface configuration command. To disable this function, use the **no** form of this command.

ip unreachable
no ip unreachable

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP *Protocol 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 kinds of ICMP unreachable messages.

Example

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

```
interface ethernet 0
 ip unreachable
```

permit

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**]

no permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]

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**]

For IGMP, you can also use the following syntax:

permit igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For TCP, you can also use the following syntax:

permit tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For UDP, you can also use the following syntax:

permit udp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**]

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP 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 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	<p>(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.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</p>

<i>icmp-message</i>	<p>(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 “Usage Guidelines” section of the access-list (extended) command.</p>
<i>igmp-type</i>	<p>(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 “Usage Guidelines” section of the access-list (extended) command.</p>
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	<p>(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 “Usage Guidelines” section of the access-list (extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.</p>
established	<p>(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.</p>
log	<p>(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.)</p> <p>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.</p> <p>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.</p>

Default

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

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

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

Example

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)
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

deny

ip access-group

ip access-list

show 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 | name]
```

Syntax Description

access-list-number (Optional) Access list number to display. The range is 0 to 1199. The system displays all access lists by default.

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

Default

The system displays all access lists.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release

Sample Display

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)
  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)
  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
  deny ip 192.150.42.0 0.0.0.255 224.0.0.0 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.

For information on how to configure access lists, refer to the “Configuring IP Services” chapter of the *Network Protocols Configuration Guide, Part 1*.

For information on how to configure dynamic access lists, refer to the “Traffic Filters Commands” chapter of the *Security Configuration Guide*.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)
access-list (standard)
clear access-list counters
clear access-temp
ip access-list
show ip access-list

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 | name]
```

Syntax Description

access-list-number (Optional) Number of the IP access list to display. This is a decimal number from 1 to 199.

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

Default

Displays all standard and extended IP access lists.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

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.

Sample Displays

The following is sample output from the **show ip access-list** command when all 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 successfully 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.

Default

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

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **output-packets** and **access-violations** keywords first appeared in Cisco IOS Release 10.3.

If you do not specify any keywords, the **show ip accounting** command displays information about the active accounting database.

To display IP access violations, you must give the **access-violations** keyword on the command. 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.

Sample Displays

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

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

Table 14 describes the fields shown in the displays.

Table 14 Show IP Accounting (and Access-Violation) Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets transmitted from the source address to the destination address. With the access-violations keyword, the number of packets transmitted from the source address to the destination address that violated an access control list.
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets transmitted from the source address to the destination address. With the access-violations keyword, the total number of bytes transmitted from the source address to the destination address that violated an access-control list.
ACL	Number of the access list of the last packet transmitted from the source to the destination that failed an access list filter.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear ip accounting

ip accounting

ip accounting-list

ip accounting-threshold

ip accounting-transits

show ip drp

To display information about the 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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Sample Display

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 15 describes the significant fields in the display.

Table 15 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

You can use the master indexes or search online to find documentation of related commands.

ip drp access-group

ip drp authentication key-chain

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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Sample Display

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 16 describes significant fields shown in the display.

Table 16 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 had 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.
bytes saved	Number of bytes reduced.

Table 16 Show IP TCP Header-Compression Field Descriptions (Continued)

Field	Description
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 had 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 small.
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

You can use the master indexes or search online to find documentation of related commands.

ip tcp header-compression

show ip traffic

To display statistics about IP traffic, use the **show ip traffic** EXEC command.

show ip traffic

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Sample Display

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

```
Router# show ip traffic

IP statistics:
  Rcvd: 98 total, 98 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
        0 fragmented, 0 couldn't fragment
  Bcast: 38 received, 52 sent
  Sent: 44 generated, 0 forwarded
        0 encapsulation failed, 0 no route

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
  Sent: 0 redirects, 3 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

UDP statistics:
  Rcvd: 56 total, 0 checksum errors, 55 no port
  Sent: 18 total, 0 forwarded broadcasts

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

EGP statistics:
  Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
  Sent: 0 total

IGRP statistics:
  Rcvd: 73 total, 0 checksum errors
  Sent: 26 total

HELLO statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
```

```
ARP statistics:
  Rcvd: 20 requests, 17 replies, 0 reverse, 0 other
  Sent: 0 requests, 9 replies (0 proxy), 0 reverse
Probe statistics:
  Rcvd: 6 address requests, 0 address replies
  0 proxy name requests, 0 other
  Sent: 0 address requests, 4 address replies (0 proxy)
      0 proxy name replies
```

Table 17 describes significant fields shown in the display.

Table 17 Show IP Traffic Field Descriptions

Field	Description
format errors	A gross error in the packet format, such as an impossible Internet header length.
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.
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.
proxy name reply	Counted when the Cisco IOS software sends an ARP or Probe Reply on behalf of another host. The display shows the number of probe proxy requests that have been received and the number of responses that have been sent.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby EXEC** command.

```
show standby [type number [group]] [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.
- brief** (Optional) A single line of output summarizes each standby group.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If you want to specify a *group*, you must also specify an interface *type* and *number*.

Sample Displays

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

```
Router# show standby

Ethernet0 - Group 0
  Local state is Active, priority 100, may preempt
  Hello time 3 holdtime 10
  Next hello sent in 0:00:00
  Hot standby IP address is 198.92.72.29 configured
  Active router is local
  Standby router is 198.92.72.21 expires in 0:00:07
  Tracking interface states for 2 interfaces, 2 up:
    Up    Ethernet0
    Up    Serial0
```

The following is sample output from the **show standby** command with a specific interface and the **brief** keyword:

```
Router# show standby ethernet0 brief

Interface  Grp Prio P State   Active addr   Standby addr   Group addr
Et0        0   100   Standby 171.69.232.33 local          172.19.48.254
```

Table 18 describes the fields in the display.

Table 18 Show Standby Field Descriptions

Field	Description
Ethernet0 - Group 0	Interface type and number and Hot Standby group number for the interface.
Local state is ...	State of local router; can be one of the following: <ul style="list-style-type: none"> • Active—Current Hot Standby router • Standby—Router next in line to be the Hot Standby router
priority	Priority value of the router based on the standby priority , standby preempt command.
may preempt (indicated by P in the brief output)	Indicates that the router will attempt to assume control as the active router if its priority is greater than the current active router.
Hello time	Time between hello packets (in seconds), based on the standby timers command.
hold time	Time (in seconds) before other routers declare the active or standby router to be down, based on the standby timers command.
Next hello sent in ...	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Hot Standby IP address is ... configured	IP address of the current Hot Standby router. The word “configured” indicates that this address is known through the standby ip command. Otherwise, the address was learned dynamically through HSRP hello packets from other routers that do have the HSRP IP address configured.
Active router is ...	Value can be “local” or an IP address. Address of the current active Hot Standby router.
Standby router is ...	Value can be “local” or an IP address. 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 interface states for ...	List of interfaces that are being tracked and their corresponding states. Based on the standby track command.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

standby authentication

standby ip

standby priority, standby preempt

standby timers

standby track

standby use-bia

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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Sample Display

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 19 describes significant fields shown in the display.

Table 19 Show TCP Statistics Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
Total	Total 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 19 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 receiver's window size.
packets after close	Number of packets received after the connection has been 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 unsent data	Number of acknowledgment packets with unsent data received.
ack packets	Number of acknowledgment packets received.
Sent	Statistics in this section refer to packets sent by the router.
Total	Total number of 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 retransmitted.
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 retransmit, but timed out.
Connections dropped in rxmit timeout	Number of connections dropped in retransmit timeout.
Keepalive timeout	Number of keepalive packets in timeout.
keepalive probe	Number of keepalive probes.
Connections dropped in keepalive	Number of connections dropped in keepalive.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear 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 string  
no standby [group-number] authentication string
```

Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which this authentication string applies.
<i>string</i>	Authentication string. It can be up to eight characters in length. The default string is cisco .

Defaults

```
group-number: 0  
string: cisco
```

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The authentication string is transmitted unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a cable to ensure interoperability. 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. Authentication mismatch does not prevent protocol events such as one router taking over as the designated router.

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

Example

In the following example, “word” is configured as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
interface ethernet 0  
  standby 1 authentication word
```

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

<i>group-number</i>	(Optional) Group number on the interface for which HSRP is being activated. Default is 0.
<i>ip-address</i>	(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

group-number: 0
HSRP is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The *group-number* argument first appeared in IOS 10.3. The **secondary** keyword first appeared in Cisco IOS 11.1.

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 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 interface's Hot Standby state is active, proxy ARP requests are answered using the Hot Standby group's MAC address. 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

In the following example, HSRP is enabled 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 Hot Standby Router Protocol (HSRP), use the **standby mac-address** interface configuration command. To revert to the standard virtual MAC address (0000.0C07.ACxy), use the **no** form of this command.

```
standby [group-number] mac-address macaddress
no standby [group-number] mac-address
```

Syntax Description

group-number (Optional) Group number on the interface for which HSRP is being activated. Default is 0.

macaddress Media Access Control (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.ACxy, where xy is the group number in hexadecimal. This address is specified in RFC 2281, Cisco Hot Standby Router Protocol (HSRP).

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command can not be used on a Token Ring Interface.

HSRP is used to help endstations locate the first hop gateway for IP routing. The endstations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as 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 as follows:

<u>APPN</u>	<u>IP</u>
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 command to configure HSRP group 1 with the virtual MAC address is as follows.

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show standby
standby use-bia

standby priority, standby preempt

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

```
standby [group-number] priority priority [preempt [delay delay]]
standby [group-number] [priority priority] preempt [delay delay]
```

```
no standby [group-number] priority priority [preempt [delay delay]]
no standby [group-number] [priority priority] preempt [delay delay]
```

Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which the other arguments in this command apply.
priority <i>priority</i>	(Optional) Priority value that prioritizes a potential Hot Standby router. The range is 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.
preempt	(Optional) 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 preempt is not configured, the local router assumes control as the active router only if it receives information indicating that there is no router currently in the active state (acting as the designated router).
delay <i>delay</i>	(Optional) Time in seconds. The <i>delay</i> argument causes the local router to postpone taking over the active role for <i>delay</i> seconds since that router was last restarted. The range is 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).

Defaults

group-number: 0

priority: 100

delay: 0 seconds; if the router wants to preempt, it will do so immediately.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

When using this command, you must specify at least one keyword (**priority** or **preempt**), or you can specify both.

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

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. This problem is solved by configuring a delay before the preempting router actually preempts the currently active router.

Example

In the following example, the router has a priority of 120 (higher than the default value) and will wait for 300 seconds (5 minutes) before attempting to become the active router:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

standby track

standby timers

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

```
standby [group-number] timers hellotime holdtime  
no standby [group-number] timers hellotime holdtime
```

Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which the timers apply. The default is 0.
<i>hellotime</i>	Hello interval in seconds. This is an integer from 1 to 255. The default is 3 seconds.
<i>holdtime</i>	Time in seconds before the active or standby router is declared to be down. This is an integer from 1 to 255. The default is 10 seconds.

Defaults

```
group-number: 0  
hellotime: 3 second  
holdtime: 10 seconds
```

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The **standby timers** command configures the time between standby hellos 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 *hellotime* ($holdtime \geq 3 * hellotime$).

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

Example

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

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

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

Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which the tracking applies.
<i>type</i>	Interface type (combined with interface number) that will be tracked.
<i>number</i>	Interface number (combined with interface type) that will be tracked.
<i>interface-priority</i>	(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

group-number: 0
interface-priority: 10

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

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

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 argument *interface-priority* specifies how much to decrement the Hot Standby priority by 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 and *interface-priority* values have been configured, these configured priority decrements are cumulative. If tracked interfaces are down, but none of them were configured with priority decrements, the default decrement is 10 and it is noncumulative.

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

Example

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

You can use the master indexes or search online to find documentation of related commands.

standby priority, standby preempt

standby use-bia

To configure Hot Standby Router Protocol (HSRP) to use the interface's burned-in address 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
no standby use-bia

Syntax Description

This command has no arguments or keywords.

Default

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

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

For an interface with this command configured, only one standby group can be configured. Multiple groups need to be removed before this command is configured. Hosts on the interface need to have a default gateway configured. It is recommended 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 HSRP routers reside on different rings, configuring the **standby use-bia** command can prevent RIF confusion.

Example

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
```

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

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

Default
Disabled

Command Mode
Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

Example

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
```

