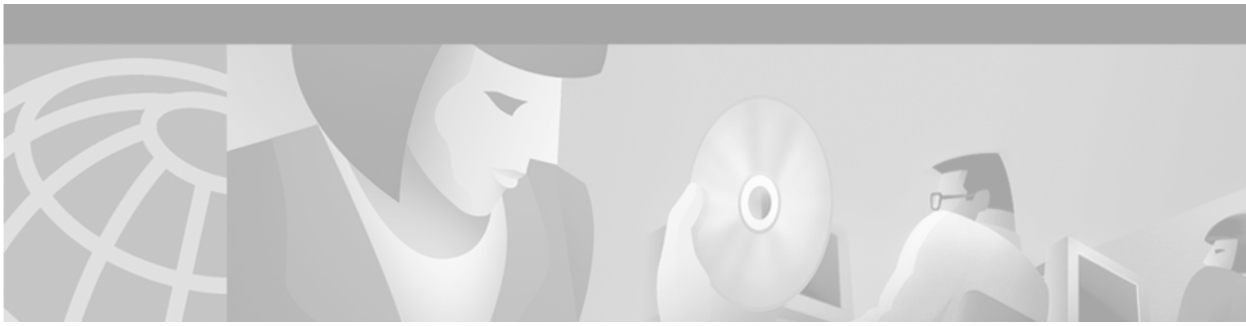

IP Services Commands

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

access-list-number	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
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.

Defaults

No access lists are defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Command	Description
show line	Displays the parameters of a terminal line.

access-list (IP 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**] [**fragments**]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

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**] [**fragments**]

Internet Group Management Protocol (IGMP)

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**] [**fragments**]

TCP

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**] [**fragments**]

User Datagram Protocol (UDP)

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**] [**fragments**]

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

access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Security Configuration Guide*.

timeout *minutes*	(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 Lock-and-Key Security (Dynamic Access Lists)” chapter in the *Security Configuration Guide*.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IP protocol. It can be one of the keywords **eigrp**, **gre, icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **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.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. 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: • 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 *source*. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0. Wildcard bits set to one do not need to be contiguous in the *source-wildcard*. For example, a *source-wildcard* of 0.255.0.64 would be valid.

destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section “Usage Guidelines.”
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the section “Usage Guidelines.”
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section “Usage Guidelines.”
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section “Usage Guidelines.”
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.

port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP 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. 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, FIN, PSH, RST, SYN or URG control 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.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command and the UDP form of this command were introduced.
10.3	The ICMP, IGMP, and TCP forms of this command were introduced. The following keywords and arguments were added: • *source* • *source-wildcard* • *destination* • *destination-wildcard* • **precedence** *precedence* • *icmp-type* • *icm-code* • *icmp-message* • *igmp-type* • *operator* • *port* • **established**
11.1	The following keywords and arguments were added: • **dynamic** *dynamic-name* • **timeout** *minutes*
11.2	The following keyword was added: • **log-input**
12.0(11)	The **fragments** keyword was added.

Usage Guidelines

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.

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**

Access List Processing of Fragments

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

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

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

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

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

Fragments and Policy Routing

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

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

Examples

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 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

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip accounting	Enables IP accounting on an interface.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

access-list (IP 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*] [**log**]

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

access-list-number	Number of an access list. This is a decimal number from1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: Use a 32-bit quantity in four-part, dotted-decimal format. Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

source-wildcard	(Optional) Wildcard bits to be applied to 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: 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 *source*. Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. Wildcard bits set to one do not need to be contiguous in the *source-wildcard*. For example, a *source-wildcard* of 0.255.0.64 would be valid.
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 source address, and the number of packets. 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.

Defaults

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 Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3(3)T	The **log** keyword was added.

Usage Guidelines

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

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP extended)	Defines an extended IP access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

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

access-list-number	Access list number of the access list for which to clear the counters.
name	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 Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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.

Examples

The following example clears the counters for access list 101:

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

Related Commands

Command	Description
show access-lists	Displays the contents of current IP and rate-limit 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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
clear ip accounting
```

Related Commands

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

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 Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example clears all DRP statistics:

```
clear ip drp
```

Related Commands

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

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 Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example clears all TCP statistics:

```
clear tcp statistics
```

Related Commands

Command	Description
show tcp statistics	Displays TCP statistics.

deny (IP)

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*] | **any**} [**log**]

no deny {*source* [*source-wildcard*] | **any**}

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

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

ICMP

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

IGMP

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

TCP

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

UDP

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

Syntax Description

source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: Use a 32-bit quantity in four-part, dotted-decimal format. Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

protocol	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.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code	(Optional) ICMP packets 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.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the "Usage Guidelines" section of the **access-list** (IP extended) command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

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 for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list 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. For both standard and extended lists, 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.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

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

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3(3)T	The **log** keyword for a standard access was added.
12.0(11)	The **fragments** keyword was added.

Usage Guidelines

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

Access List Processing of Fragments

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

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

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

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

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

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

Fragments and Policy Routing

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

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

Examples

The following example sets 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

Command	Description
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
permit (IP)	Sets conditions for a named IP access list.
show access-lists	Displays the contents of all current IP access lists.

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**] [**fragments**]

no dynamic *dynamic-name*

ICMP

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**] [**fragments**]

IGMP

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

TCP

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**] [**fragments**]

UDP

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**] [**fragments**]

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

Syntax Description

dynamic-name	Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Security Configuration Guide*.
timeout *minutes*	(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 Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Security Configuration Guide*.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

protocol	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.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section “Usage Guidelines.”
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the section “Usage Guidelines.”
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code	(Optional) ICMP packets 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.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
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.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

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

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11)	The **fragments** keyword was added.

Usage Guidelines

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**

Access List Processing of Fragments

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

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

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

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

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

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

Fragments and Policy Routing

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

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

Examples

The following example defines a dynamic access list named washington:

```
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

Command	Description
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

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

access-list-number	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
name	Name of an IP access list as specified by an **ip access-list** command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *name* argument was added.

Usage Guidelines

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).

Examples

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

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

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of current IP and rate-limit 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.
name	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.

Defaults

No named IP access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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.

Examples

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

Command	Description
deny (IP)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
permit (IP)	Sets conditions for a named IP access list.
show access-lists	Displays the contents of all current IP access lists.

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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **access-violations** keyword was added.

Usage Guidelines

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.

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), you must include the **log** keyword in the **access-list** (IP extended) or **access-list** (IP standard) command.

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

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

Examples

The following example enables IP accounting on Ethernet interface 0:

```
interface ethernet 0
 ip accounting
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-list

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** 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

ip-address	IP address in dotted-decimal format.
wildcard	Wildcard bits to be applied to *ip-address*.

Defaults

No filters are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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.

Examples

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

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

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-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.

Defaults

512 entries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
ip accounting-threshold 500
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-transits

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

ip accounting-transits *count*

no ip accounting-transits

Syntax Description

count	Number of transit records to store in the IP accounting database.

Defaults

0

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
ip accounting-transits 100
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting mac-address

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

ip accounting mac-address {**input** | **output**]

no ip accounting mac-address {**input** | **output**]

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.

Usage Guidelines

This feature is supported on Ethernet, FastEthernet, and FDDI interfaces.

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

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

Examples

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

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

Related Commands

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

ip accounting precedence

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

ip accounting precedence {**input** | **output**]

no ip accounting precedence {**input** | **output**]

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip 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 or from 1300 to 1999.

Defaults

The DRP Server Agent will answer all queries.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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.

Examples

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

Command	Description
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

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.

Defaults

No authentication is configured for the DRP Server Agent.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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.

Examples

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

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

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.
show key chain	Displays authentication key information.

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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example enables the DRP Server Agent:

```
ip drp server
```

Related Commands

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

ip icmp rate-limit unreachable

To have the Cisco IOS software limit the rate that Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **ip icmp rate-limit unreachable** global configuration command. To remove the rate limit, use the **no** form of this command.

ip icmp rate-limit unreachable [**df**] *milliseconds*

no ip icmp rate-limit unreachable [**df**]

Syntax Description

df	(Optional) Limits the rate ICMP destination unreachable messages are sent when code 4, fragmentation is needed and DF set, is specified in the IP header of the ICMP destination unreachable message.
milliseconds	Time limit (in milliseconds) in which one ICMP destination unreachable message is sent. The range is 1 millisecond to 4294967295 milliseconds.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

The following example turns off the previously configured rate limit:

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

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

```
default ip icmp rate-limit unreachable
```

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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

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.

Defaults

Minimum is 128 bytes; maximum depends on interface medium.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Note

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

Examples

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

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

Related Commands

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

ip redirects

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

ip redirects

no ip redirects

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled, unless Hot Standby Router Protocol is configured

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If the Hot Standby Router Protocol is configured on an interface, ICMP Redirect messages are disabled by default for the interface.

Examples

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

```
interface ethernet 0
 ip redirects
```

Related Commands

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

ip source-route

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

ip source-route

no ip source-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
ip source-route
```

Related Commands

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

ip tcp chunk-size

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

ip tcp chunk-size *characters*

no ip tcp chunk-size

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.

Usage Guidelines

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

Examples

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

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

ip tcp compression-connections

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

ip tcp compression-connections *number*

no ip tcp compression-connections *number*

Syntax Description

number	Number of connections the cache supports. It can be a number from 3 to 256.

Defaults

16 connections

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ip tcp header-compression

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

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

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

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, the Cisco IOS software compresses all traffic.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC or 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.

Examples

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

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

Related Commands

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

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** global configuration command. To disable the function, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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.

Examples

The following example enables Path MTU Discovery:

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

ip tcp queuemax

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

ip tcp queuemax *packets*

no ip tcp queuemax

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
ip tcp queuemax 10
```

ip tcp selective-ack

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

ip tcp selective-ack

no ip tcp selective-ack

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round trip time. An aggressive sender could 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.

Examples

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

```
ip tcp selective-ack
```

Related Commands

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

ip tcp synwait-time

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

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Syntax Description

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

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In versions previous to Cisco IOS software 10.0, the system would wait a fixed 30 seconds when attempting to establish a TCP connection. If your network contains Public Switched Telephone Network (PSTN) dial-on-demand routing (DDR), the call setup time may exceed 30 seconds. This amount of time is not sufficient in networks that have 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.

Examples

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

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

ip tcp timestamp

To enable TCP 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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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.

Examples

The following example enables the router to send TCP timestamps:

```
ip tcp timestamp
```

Related Commands

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

ip tcp window-size

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

ip tcp window-size *bytes*

no ip tcp window-size

Syntax Description

bytes	Window size in bytes. The maximum is 65535 bytes. The default value is 2144 bytes.

Defaults

2144 bytes

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

ip unreachables

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

ip unreachables

no ip unreachables

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
interface ethernet 0
 ip unreachables
```

permit (IP)

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

permit {*source* [*source-wildcard*] | **any**} [**log**]

no permit {*source* [*source-wildcard*] | **any**}

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**] [**fragments**]

ICMP

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

IGMP

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

TCP

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

UDP

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

Syntax Description

source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: Use a 32-bit quantity in four-part, dotted-decimal format. Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: 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 *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

protocol	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.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the "Usage Guidelines" section of the **access-list (IP extended)** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code	(Optional) ICMP packets 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.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “Usage Guidelines” section of the **access-list (IP extended)** command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the **access-list (IP extended)** command.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the **access-list (IP extended)** command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

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 for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list 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. For both standard and extended lists, 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.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the “Access List Processing of Fragments” and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.

Defaults

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

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3(3)T	The **log** keyword for a standard access list was added.
12.0(11)	The **fragments** keyword was added.

Usage Guidelines

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

Access List Processing of Fragments

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

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

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

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

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

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

Fragments and Policy Routing

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

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

Examples

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

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

Related Commands

Command	Description
deny (IP)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of all current IP access lists.

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

Defaults

The system displays all access lists.

Command Modes

Privileged EXEC

Examples

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

```
Router# show access-lists 101
Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches)
    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 Filtering and Firewalls” chapter of the *Security Configuration Guide*.

Related Commands

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

show interface mac

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

show interface precedence

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

show ip access-list

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

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

Syntax Description

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

Defaults

Displays all standard and extended IP access lists.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

Examples

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

Defaults

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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added: • **output-packets** • **access-violations**

Usage Guidelines

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.

Examples

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

```
Router# show ip accounting

   Source           Destination              Packets               Bytes
 131.108.19.40    192.67.67.20                     7                 306
 131.108.13.55    192.67.67.20                    67                2749
 131.108.2.50     192.12.33.51                    17                1111
 131.108.2.50     130.93.2.1                       5                 319
 131.108.2.50     130.93.1.2                     463               30991
 131.108.19.40    130.93.2.1                       4                 262
 131.108.19.40    130.93.1.2                      28                2552
 131.108.20.2     128.18.6.100                    39                2184
 131.108.13.55    130.93.1.2                      35                3020
 131.108.19.40    192.12.33.51                  1986               95091
 131.108.2.50     192.67.67.20                   233               14908
 131.108.13.28    192.67.67.53                   390               24817
 131.108.13.55    192.12.33.51                214669             9806659
 131.108.13.111   128.18.6.23                  27739             1126607
 131.108.13.44    192.12.33.51                 35412             1523980
 192.31.7.21      130.93.1.2                      11                 824
 131.108.13.28    192.12.33.2                     21                1762
 131.108.2.166    192.31.7.130                   797              141054
 131.108.3.11     192.67.67.53                     4                 246
 192.31.7.21      192.12.33.51                 15696              695635
 192.31.7.24      192.67.67.20                    21                 916
 131.108.13.111   128.18.10.1                     16                1137
 accounting threshold exceeded for 7 packets and 433 bytes
```

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

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
131.108.19.40    192.67.67.20              7          306         77
131.108.13.55    192.67.67.20             67         2749        185
131.108.2.50     192.12.33.51             17         1111        140
131.108.2.50     130.93.2.1                5          319        140
131.108.19.40    130.93.2.1                4          262         77
Accounting data age is 41
```

Table 11 describes the fields shown in the displays.

Table 11 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.

Table 11 show ip accounting (and access-violation) Field Descriptions (continued)

Field	Description
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.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.

Related Commands

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

show ip 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 Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

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

```
Router# show ip drp
Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using “test” key-chain
```

Table 12 describes the significant fields in the display.

Table 12 show ip drp Field Descriptions

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

Related Commands

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

show ip redirects

To display the address of a default gateway (router) and the address of hosts for which an ICMP Redirect messages has been received, use the **show ip redirects** EXEC command.

show ip redirects

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

The **ip redirects** command enables the router to send ICMP Redirect messages.

Examples

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

```
Router# show ip redirects

Default gateway is 160.89.80.29

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

Related Commands

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

show ip sockets

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

show ip sockets

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC
User EXEC

Command History

Release	Modification
10.0 T	This command was introduced.

Usage Guidelines

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

Examples

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

```
Router# show ip sockets

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

Table 13 describes the significant fields shown in the display.

Table 13 show ip sockets Field Descriptions

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

show ip tcp header-compression

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

show ip tcp header-compression

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show ip tcp header-compression

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

Table 14 describes significant fields shown in the display.

Table 14 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.

Table 14 show ip tcp header-compression Field Descriptions (continued)

Field	Description
bytes saved	Number of bytes reduced.
bytes sent	Number of bytes sent.
efficiency improvement factor	Improvement in line efficiency because of TCP header compression.
Connect:	
slots	Size of the cache.
long searches	Indicates the number of times the software 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

Command	Description
ip tcp header-compression	Enables 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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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 15 describes significant fields shown in the display.

Table 15 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.

Table 15 show ip traffic Field Descriptions (continued)

Field	Description
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 Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

```
Router# show standby

Ethernet0 - Group 0
  Local state is Active, priority 100, may preempt
  Hellotime 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 16 describes the fields in the display.

Table 16 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: • 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.
Hellotime	Time between hello packets (in seconds), based on the **standby timers** command.
holdtime	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

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby priority, standby preempt	Configures HSRP priority, preemption, and preemption delay.
standby timers	Configures the time between hellos and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show tcp statistics

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

show tcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

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

```
Router# show tcp statistics

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

Table 17 describes significant fields shown in the display.

Table 17 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.

Table 17 show tcp statistics Field Descriptions (continued)

Field	Description
bad offset	Number of packets received with bad offset to data.
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

Command	Description
clear tcp statistics	Clears TCP statistics.

standby authentication

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

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

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

Syntax Description

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

Defaults

group-number: 0
string: **cisco**

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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 interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP. 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.

The authentication string has a lower priority than the priority set with the **standby priority** command. A router with a higher HSRP priority will ignore the authentication string.

Examples

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

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

Related Commands

Command	Description
standby priority, standby preempt	Configures HSRP priority, preemption, and preemption delay.

standby ip

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

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

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

Syntax Description

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

Defaults

group-number: 0

HSRP is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

standby mac-address

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

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

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

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
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.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, Cisco Hot Standby Router Protocol (HSRP).

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command 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:

APPN	IP
end node	host
network node	router or gateway

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

Examples

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

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

Related Commands

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

standby mac-refresh

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

standby mac-refresh *seconds*

no standby mac-refresh

Syntax Description

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

Defaults

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
standby mac-refresh 100
```

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

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
priority *priority*	(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 *delay*	(Optional) Time in seconds. The *delay* argument causes the local router to postpone taking over the active role for *delay* 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 Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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.

The assigned priority has a higher priority than the authentication string specified in the **standby authentication** command. A router with a higher HSRP priority will ignore the authentication string.

Examples

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

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

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** [**msec**] *hellotime* [**msec**] *holdtime*

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

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply. The default is 0.
msec	(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
hellotime	Hello interval in seconds.This is an integer from 1 to 255. The default is 3 seconds. If the **msec** option is specified, hello interval is in milliseconds. This is an integer from 20 to 999.
holdtime	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. If the **msec** option is specified, holdtime is in milliseconds. This is an integer from 20 to 999.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **msec** keyword was added.

Usage Guidelines

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 the value of hellotime, ($holdtime \geq 3 * hellotime$).

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

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

Examples

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

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

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

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

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

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

Defaults

group-number: 0

interface-priority: 10

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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.

Examples

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

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

Related Commands

Command	Description
standby priority, standby preempt	Configures HSRP priority, preemption, and preemption delay.

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.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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 HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent RIF confusion.

Examples

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

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

transmit-interface

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

transmit-interface *type number*

no transmit-interface

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

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