



IP Addressing and Services Commands

access-class

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

```
access-class access-list-number { in [vrf-also] | out }
```

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

Syntax Description

<i>access-list-number</i>	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.
vrf-also	Accepts incoming connections from interfaces that belong to a VRF.
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.
12.2	The vrf-also keyword was added.

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.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

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** command in global configuration mode. 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] [time-range time-range-name] [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-code] |
  icmp-message] [precedence precedence] [tos tos] [log | log-input] [time-range
  time-range-name] [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] [time-range time-range-name]
  [fragments]
```

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

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

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic <i>dynamic-name</i>	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Cisco IOS Security Configuration Guide</i> .
timeout <i>minutes</i>	(Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Cisco IOS Security Configuration Guide</i> .

deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an Internet protocol. It can be one of the keywords eigrp , gre , icmp , igmp , ip , ipinip , nos , ospf , pim , tcp , or udp , or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the ip keyword. Some protocols allow further qualifiers described below.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. <p>There are three alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. <p>Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.</p>
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the any keyword as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

precedence <i>precedence</i>	(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 <i>tos</i>	(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.”
log	<p>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)</p> <p>The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.</p> <p>The logging facility may drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.</p>
log-input	(Optional) Includes the input interface and source MAC address or VC in the logging output.
time-range <i>time-range-name</i>	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the time-range command.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section “Usage Guidelines.”
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section “Usage Guidelines.”
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>

<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section “Usage Guidelines.” TCP port names can only be used when filtering TCP. 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 or RST control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the “ Access List Processing of Fragments ” and “ Fragments and Policy Routing ” sections in the “Usage Guidelines” section.

Defaults

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 was introduced.
10.3	The following keywords and arguments were added: <ul style="list-style-type: none"> • <i>source</i> • <i>source-wildcard</i> • <i>destination</i> • <i>destination-wildcard</i> • precedence <i>precedence</i> • <i>icmp-type</i> • <i>icmp-code</i> • <i>icmp-message</i> • <i>igmp-type</i> • <i>operator</i> • <i>port</i> • established
11.1	The dynamic <i>dynamic-name</i> keyword and argument were added.
11.1	The timeout <i>minutes</i> keyword and argument were added.
11.2	The log-input keyword was added.
12.0(1)T	The time-range <i>time-range-name</i> keyword and argument were added.

Release	Modification
12.0(11)	The fragments keyword was added.
12.2(13)T	The non500-isakmp keyword was added to the list of UDP port names. The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.

Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the 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 vty access or restrict the contents of routing updates must not match against the TCP source port, the type of service (ToS) value, or the precedence of the packet.



Note

After a numbered access list is created, 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 numbered 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 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 if you type 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 if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **non500-isakmp**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xmcp**

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..
<p>...no fragments keyword (the default behavior), and assuming all of the access-list entry information matches,</p>	<p>For an access-list entry containing only Layer 3 information:</p> <ul style="list-style-type: none"> • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. <p>For an access list entry containing Layer 3 and Layer 4 information:</p> <ul style="list-style-type: none"> • The entry is applied to nonfragmented packets and initial fragments. <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 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. <p> Note The deny statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</p>
<p>...the fragments keyword, and assuming all of the access-list entry information matches,</p>	<p>The access-list entry is applied only to noninitial fragments.</p> <p> Note The fragments keyword cannot be configured for an access-list entry that contains any Layer 4 information.</p>

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

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

**Note**

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

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** 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 address of the mail host is 128.88.1.2. The **established** keyword 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 indicates 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 permits 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. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.108.0.0 255.255.0.0 but denies 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
```

The following example permits 131.108.0/24 but denies 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
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
 !
access-list 101 deny tcp any any eq http time-range no-http
 !
interface ethernet 0
 ip access-group 101 in
```

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.
	access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
	clear access-template	Clears a temporary access list entry from a dynamic access list.
	delay (tracking)	Sets conditions under which a packet does not pass a named 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.
	ip access-list	Defines an IP access list by name.
	ip accounting	Enables IP accounting on an interface.
	logging console	Controls which messages are logged to the console, based on severity.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
	permit (IP)	Sets conditions under which a packet passes a named access list.
	remark	Writes a helpful comment (remark) for an entry in a named IP access list.
	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.
	time-range	Specifies when an access list or other feature is in effect.

access-list (IP standard)

To define a standard IP access list, use the standard version of the **access-list** command in global configuration mode. 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
```

Syntax Description	
<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>source</i>	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part, dotted-decimal format. Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
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 vty 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.

**Caution**

Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS 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 condition could cause you severe security problems.** Save your old configuration file before booting these images.

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 from 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.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.

Command	Description
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark (IP)	Writes a helpful comment (remark) for an entry in a named IP access list.
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 compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **access-list compiled** command in global configuration mode. To disable the Turbo ACL feature, use the **no** form of this command.

access-list compiled

no access-list compiled

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

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

Usage Guidelines

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the **access-list compiled** command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

Examples

The following example enables the Turbo ACL feature:

```
access-list compiled
```

access-list remark

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

access-list *access-list-number* **remark** *remark*

no access-list *access-list-number* **remark** *remark*

Syntax Description		
	<i>access-list-number</i>	Number of an IP access list.
	<i>remark</i>	Comment that describes the access list entry, up to 100 characters long.

Defaults The access list entries have no remarks.

Command Modes Global configuration

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

Usage Guidelines The remark can be up to 100 characters long; anything longer is truncated.
If you want to write a comment about an entry in a named access list, use the **remark** command.

Examples In the following example, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
access-list 1 remark Permit only Jones workstation through
access-list 1 permit 171.69.2.88
access-list 1 remark Do not allow Smith workstation through
access-list 1 deny 171.69.3.13
```

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.
	remark	Writes a helpful comment (remark) for an entry in a named IP access list.

accounting (DHCP)

To enable DHCP accounting, use the **accounting** command in DHCP pool configuration mode. To disable DHCP accounting for the specified server group, use the **no** form of this command.

accounting *server-group-name*

no accounting *server-group-name*

Syntax Description	<i>server-group-name</i>	Name of a server group to apply DHCP accounting. The server group can have one or more members. The server group is defined in the configuration of the aaa group server and aaa accounting commands.
---------------------------	--------------------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	DHCP pool configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines

The **accounting** DHCP pool configuration command is used to enable the DHCP accounting feature by sending secure DHCP START accounting messages when IP addresses are assigned to DHCP clients, and secure DHCP STOP accounting messages when DHCP leases are terminated. A DHCP lease is terminated when the client explicitly releases the lease, when the session times out, and when the DHCP bindings are cleared from the DHCP database. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

The **accounting** command can be used only to network pools in which bindings are created automatically and destroyed upon lease termination (or when the client sends a DHCP RELEASE message). DHCP bindings are also destroyed when the **clear ip dhcp binding** or **no service dhcp** command is issued. These commands should be used with caution if an address pool is configured with DHCP accounting.

AAA and RADIUS must be configured before this command can be used to enable DHCP accounting. A server group must be defined with the **aaa group server** command. START and STOP message generation is configured with the **aaa accounting** command. The **aaa accounting** command can be configured to enable the DHCP accounting to send both START and STOP messages or STOP messages only.

Examples

The following example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group.

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# accounting RADIUS-GROUP1
Router(dhcp-config)# exit
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
aaa session-id	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that IOS will look for RADIUS server hosts.
service dhcp	Enables the Cisco IOS DHCP server and relay agent features.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.
update arp	Secures the MAC address of the authorized client interface to the DHCP binding.

advertise

To control the installation of a static route to the Null0 interface for a virtual server address, use the **advertise** SLB virtual server configuration command. To prevent the installation of a static route for the virtual server IP address, use the **no** form of this command.

advertise

no advertise

Syntax Description This command has no arguments or keywords.

Defaults The SLB virtual server IP address is added to the routing table.

Command Modes SLB virtual server configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines By default, virtual server addresses are *advertised*. That is, static routes to the Null0 interface are installed for the virtual server addresses.

Advertisement of this static route using the routing protocol requires that you configure redistribution of static routes for the routing protocol.

Examples The following example prevents advertisement of the IP address of the virtual server in routing protocol updates:

```
ip slb vserver PUBLIC_HTTP
no advertise
```

Related Commands	Command	Description
	show ip slb vservers	Displays information about the virtual servers.

agent

To configure a Dynamic Feedback Protocol (DFP) agent, use the **agent** SLB command in DFP configuration mode. To remove an agent definition from the DFP configuration, use the **no** form of this command.

```
agent ip-address port [timeout [retry-count [retry-interval]]]
```

```
no agent ip-address port
```

Syntax Description	
<i>ip-address</i>	Agent IP address.
<i>port</i>	Agent port number.
<i>timeout</i>	(Optional) Time period (in seconds) during which the DFP manager must receive an update from the DFP agent. The default is 0 seconds, which means there is no timeout.
<i>retry-count</i>	(Optional) Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. The default is 0 retries, which means there are infinite retries.
<i>retry-interval</i>	(Optional) Interval (in seconds) between retries. The default is 180 seconds.

Defaults

The default timeout is 0 seconds (no timeout).
 The default retry count is 0 (infinite retries).
 The default retry interval is 180 seconds.

Command Modes

SLB DFP configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

You can configure up to 1024 agents.

A DFP agent collects status information about the load capability of a server and reports that information to a load manager. The DFP agent may reside on the server, or it may be a separate device that collects and consolidates the information from several servers before reporting to the load manager.

Examples

The following example configures a DFP agent on the DFP manager, sets the DFP password to *Cookies* and the timeout to *360* seconds, changes the configuration mode to DFP configuration mode, sets the IP address of the DFP agent to *10.1.1.1*, and sets the port number of the DFP agent to *2221* (FTP):

```
ip slb dfp password Cookies 360
agent 10.1.1.1 2221
```

■ agent

Related Commands

Command	Description
ip slb dfp	Configures the IOS SLB DFP.

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode. To remove an entry from the ARP cache, use the **no** form of this command.

```
arp {ip-address | vrf vrf-name} hardware-address encap-type [interface-type]
```

```
no arp {ip-address | vrf vrf-name} hardware-address encap-type [interface-type]
```

Syntax Description	
<i>ip-address</i>	IP address in four-part dotted decimal format corresponding to the local data-link address.
vrf <i>vrf-name</i>	Virtual Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument is the name of the VRF table.
<i>hardware-address</i>	Local data-link address (a 48-bit address).
<i>encap-type</i>	Encapsulation description. The keywords are as follows: <ul style="list-style-type: none"> • arpa—For Ethernet interfaces. • sap—For Hewlett Packard interfaces. • smds—For Switched Multimegabit Data Service (SMDS) interfaces. • snap—For FDDI and Token Ring interfaces. • srp-a—Switch Route Processor, side A (SRP-A) interfaces. • srp-b—Switch Route Processor, side B (SRP-B) interfaces.
<i>interface-type</i>	(Optional) Interface type. The keywords are as follows: <ul style="list-style-type: none"> • ethernet—IEEE 802.3 interface. • loopback—Loopback interface. • null—No interface. • serial—Serial interface. • alias—Cisco IOS software responds to ARP requests as if it were the interface of the specified address.

Defaults No entries are permanently installed in the ARP cache.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 10.31.7.19 0800.0900.1834 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.

arp (interface)

To control the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, Frame Relay, and Token Ring hardware addresses, use the **arp** command in interface configuration mode. To disable an encapsulation type, use the **no** form of this command.

```
arp { arpa | frame-relay | snap }
```

```
no arp { arpa | frame-relay | snap }
```

Syntax Description	Command	Description
	arpa	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
	frame-relay	Enables ARP over a Frame Relay encapsulated interface.
	snap	ARP packets conforming to RFC 1042.

Defaults Standard Ethernet-style ARP

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(13)T	The probe keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.

Usage Guidelines Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of ARP.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces EXEC** command displays the type of ARP being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples The following example enables frame relay services:

```
interface ethernet 0
  arp frame-relay
```

Related Commands	Command	Description
	clear arp-cache	Deletes all dynamic entries from the ARP cache.
	show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp timeout

To configure how long an entry remains in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description	<i>seconds</i>	Time (in seconds) that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.
---------------------------	----------------	--

Defaults	14400 seconds (4 hours)
-----------------	-------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command is ignored when issued on interfaces that do not use ARP. The **show interfaces EXEC** command displays the ARP timeout value. The value follows the “Entry Timeout:” heading, as seen in the following example from the **show interfaces** command:

```
ARP type: ARPA, PROBE, Entry Timeout: 14400 sec
```

Examples The following example sets the ARP timeout to 12000 seconds to allow entries to time out more quickly than the default:

```
interface ethernet 0
  arp timeout 12000
```

Related Commands	Command	Description
	show interfaces	Displays statistics for all interfaces configured on the router or access server.

bindid

To configure a bind ID, use the **bindid** command in SLB server farm configuration mode. To remove a bind ID from the server farm configuration, use the **no** form of this command.

bindid [*bind-id*]

no bindid [*bind-id*]

Syntax Description	<i>bind-id</i> (Optional) Bind ID number. The default bind ID is 0.
---------------------------	---

Defaults	The default bind ID is 0.
-----------------	---------------------------

Command Modes	SLB server farm configuration
----------------------	-------------------------------

Command History	Release	Modification
	12.0(7)XE	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	<p>You can configure one bind ID on each bindid command.</p> <p>The bind ID allows a single physical server to be bound to multiple virtual servers and report a different weight for each one. Thus, the single real server is represented as multiple instances of itself, each having a different bind ID. DFP uses the bind ID to identify for which instance of the real server a given weight is specified.</p>
-------------------------	--

Examples	The following example configures bind ID 309:
-----------------	---

```
ip slb serverfarm PUBLIC
bindid 309
```

Related Commands	Command	Description
	ip slb dfp	Configures the IOS SLB DFP.

bootfile

To specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client, use the **bootfile** command in DHCP pool configuration mode. To delete the boot image name, use the **no** form of this command.

bootfile *filename*

no bootfile

Syntax Description	<i>filename</i>	Specifies the name of the file that is used as a boot image.
--------------------	-----------------	--

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	DHCP pool configuration
---------------	-------------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Examples	The following example specifies xllboot as the name of the boot file:
----------	---

```
bootfile xllboot
```

Related Commands	Command	Description
	ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
	next-server	Configures the next server in the boot process of a DHCP client.

clear access-list counters

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

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

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

Command Modes Privileged 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:

```
Router# clear access-list counters 101
```

Related Commands	Command	Description
	show access-lists	Displays the contents of current IP and rate-limit access lists.

clear arp interface

To clear the entire Address Resolution Protocol (ARP) cache on an interface, use the **clear arp interface** command in EXEC mode.

clear arp interface *type number*

Syntax Description	<i>type</i>	Interface type.
	<i>number</i>	Interface number.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines Use the **clear arp interface** command to clean up ARP entries associated with an interface.

Examples The following example clears the ARP cache from Ethernet interface 0:

```
Router# clear arp interface ethernet 0
```

clear arp-cache

To delete all dynamic entries from the Address Resolution Protocol (ARP) cache, to clear the fast-switching cache, and to clear the IP route cache, use the **clear arp-cache** command in EXEC mode.

clear arp-cache

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 example removes all dynamic entries from the ARP cache and clears the fast-switching cache:

```
clear arp-cache
```

Related Commands	Command	Description
	arp (global)	Adds a permanent entry in the ARP cache.
	arp (interface)	Controls the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, and Token Ring hardware addresses.

clear host

To delete entries from the host name-to-address cache, use the **clear host** EXEC command.

clear host {*name* | *}

Syntax Description

<i>name</i>	Particular host entry to remove.
*	Removes all entries.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The host name entries will not be removed from NVRAM, but will be cleared in running memory.

Examples

The following example clears all entries from the host name-to-address cache:

```
clear host *
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

clear ip accounting

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

clear ip accounting [checkpoint]

Syntax Description	checkpoint (Optional) Clears the checkpointed database.
---------------------------	--

Command Modes	Privileged 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:
-----------------	---

```
Router> 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-transit	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 dhcp binding

To delete an automatic address binding from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** command in privileged EXEC mode.

```
clear ip dhcp [pool name] binding {* | address}
```

Syntax Description

pool name	(Optional) Name of the DHCP pool.
*	Clears all automatic bindings.
<i>address</i>	The address of the binding you want to clear.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	The pool name keyword and argument combination was added.

Usage Guidelines

Typically, the address denotes the IP address of the client. If the asterisk (*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp pool** global configuration command to delete a manual binding.

Note the following behavior for the **clear ip dhcp binding** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified binding.
- If you do not specify the **pool name** option and the * option is specified, it is assumed that all automatic or on-demand bindings in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the * option, all automatic or on-demand bindings in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified binding will be deleted from the specified pool.

Examples

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

The following example deletes all bindings from all pools:

```
Router# clear ip dhcp binding *
```

The following example deletes all bindings from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 binding *
```

The following example deletes address binding 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool red binding pool2
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

clear ip dhcp conflict

To clear an address conflict from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp conflict** command in privileged EXEC mode.

```
clear ip dhcp [pool name] conflict [* | address]
```

Syntax Description	pool name	(Optional) Name of the DHCP pool.
	*	Clears all address conflicts.
	<i>address</i>	The IP address of the host that contains the conflicting address you want to clear.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(8)T	The pool name keyword and argument combination were added.

Usage Guidelines The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (*) character is used as the address parameter, DHCP clears all conflicts.

Note the following behavior for the **clear ip dhcp conflict** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified conflict.
- If you do not specify the **pool name** option and the * option is specified, it is assumed that all automatic/ or on-demand conflicts in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the * option, all automatic or on-demand conflicts in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified conflict will be deleted from the specified pool.

Examples The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

The following example deletes all address conflicts from all pools:

```
Router# clear ip dhcp conflict *
```

The following example deletes all address conflicts from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 conflict *
```

The following example deletes address conflict 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 conflict 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

clear ip dhcp server statistics

To reset all Cisco IOS Dynamic Host Configuration Protocol (DHCP) server counters, use the **clear ip dhcp server statistics** command in privileged EXEC mode.

clear ip dhcp server statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines The **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters will be initialized, or set to zero, with the **clear ip dhcp server statistics** command.

Examples The following example resets all DHCP counters to zero:

```
Router# clear ip dhcp server statistics
```

Related Commands	Command	Description
	show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.

clear ip dhcp subnet

To clear all currently leased subnets in the Cisco IOS Dynamic Host Configuration Protocol (DHCP) pool, use the **clear ip dhcp subnet** command in privileged EXEC configuration mode.

```
clear ip dhcp [pool name] subnet { * | address }
```

Syntax Description	pool name	(Optional) Name of the DHCP pool.
	*	Clears all leased subnets.
	address	Clears a subnet containing the specified IP address.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines A PPP session that is allocated an IP address from the released subnet will be reset.

Note the following behavior for the **clear ip dhcp subnet** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified subnet.
- If you do not specify the **pool name** option and the * option is specified, it is assumed that all automatic or on-demand subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the * option, all automatic or on-demand subnets in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the subnet containing the specified IP address will be deleted from the specified pool.



Caution

Use this command with caution to prevent undesired termination of active PPP sessions.

Examples

The following example releases the subnet containing 10.0.0.2 from any non-VRF on-demand address pools:

```
Router# clear ip dhcp subnet 10.0.0.2
```

The following example clears all leased subnets from all pools:

```
Router# clear ip dhcp subnet *
```

The following example clears all leased subnets from the address pool named pool3:

```
Router# clear ip dhcp pool pool3 subnet *
```

clear ip dhcp subnet

The following example clears the address 10.0.0.2 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 subnet 10.0.0.2
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

clear ip drp

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

clear ip drp

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

Examples The following example clears all DRP statistics:

```
Router> 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 ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in EXEC mode.

```
clear ip nat translation [* | [inside global-ip global-port local-ip local-port] | [outside local-ip global-ip]]
```

```
clear ip nat translation [esp | tcp | udp] [inside global-ip global-port local-ip local-port] | [outside local-ip global-ip]
```

Syntax Description		
	*	Clears all dynamic translations.
	inside	(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
	<i>global-ip</i>	(Optional) Global IP address.
	<i>global-port</i>	(Optional) Global port.
	<i>local-ip</i>	(Optional) Local IP address.
	<i>local-port</i>	(Optional) Local port.
	outside	(Optional) Clears the outside translations containing the specified <i>global</i> and <i>local</i> addresses.
	esp	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
	tcp	(Optional) Clears the TCP entries from the translation table.
	udp	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.

Command Modes	
	EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	The esp keyword was added.

Usage Guidelines	
	Use this command to clear entries from the translation table before they time out.

Examples	
	The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router> show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

```
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
```

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** EXEC command.

clear ip nhrp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines This command does not clear any static (configured) IP-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

Examples The following example clears all dynamic entries from the NHRP cache for the interface:

```
clear ip nhrp
```

Related Commands	Command	Description
	show ip nhrp	Displays the NHRP cache.

clear ip route dhcp

To remove routes from the routing table added by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent for the DHCP clients on unnumbered interfaces, use the **clear ip route dhcp** command in EXEC mode.

```
clear ip route [vrf vrf-name] dhcp [ip-address]
```

Syntax Description	Parameter	Description
	vrf	(Optional) VPN routing and forwarding instance (VRF).
	<i>vrf-name</i>	(Optional) Name of the VRF.
	<i>ip-address</i>	(Optional) Address about which routing information should be removed.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.2	This command was introduced.

Usage Guidelines To remove information about global routes in the routing table, use the **clear ip route dhcp** command. To remove routes in the VRF routing table, use the **clear ip route vrf vrf-name dhcp** command.

Examples The following example removes a route to network 55.5.5.217 from the routing table:

```
Router# clear ip route dhcp 55.5.5.217
```

Related Commands	Command	Description
	show ip route dhcp	Displays the routes added to the routing table by the Cisco IOS DHCP server and relay agent.

clear ip route

To delete routes from the IP routing table, use the **clear ip route** EXEC command.

clear ip route {*network* [*mask*] | *}

Syntax Description

<i>network</i>	Network or subnet address to remove.
<i>mask</i>	(Optional) Subnet address to remove.
*	Removes all routing table entries.

Defaults

All entries are removed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example removes a route to network 132.5.0.0 from the IP routing table:

```
clear ip route 132.5.0.0
```

clear ip slb

To clear IP IOS SLB connections or counters, use the **clear ip slb** privileged EXEC command.

```
clear ip slb {connections [serverfarm farm-name | vserver server-name] | counters}
```

Syntax Description	connections	Clears the IP IOS SLB connection database.
	serverfarm	(Optional) Clears the connection database for the server farm named.
	<i>farm-name</i>	(Optional) Character string used to identify the server farm.
	vserver	(Optional) Clears the connection database for the virtual server named.
	<i>server-name</i>	(Optional) Character string used to identify the virtual server.
	counters	Clears the IP IOS SLB counters.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example clears the connection database of the server farm named FARM1:

```
Router# clear ip slb connections serverfarm FARM1
```

The following example clears the connection database of the virtual server named VSERVER1:

```
Router# clear ip slb connections vserver VSERVER1
```

The following example clears the IOS SLB counters:

```
Router# clear ip slb counters
```

Related Commands	Command	Description
	show ip slb conns	Displays information about the IOS SLB connections.
	show ip slb serverfarms	Displays information about the IOS SLB server farms.
	show ip slb vservers	Displays information about the IOS SLB virtual servers.

clear ip snat sessions

To clear dynamic Stateful Network Address Translation (SNAT) sessions from the translation table, use the **clear ip snat sessions** command in EXEC mode.

```
clear ip snat sessions * [ip-address-peer]
```

Syntax Description	*	Removes all dynamic entries.
	<i>ip-address-peer</i>	(Optional) Removes SNAT entries of the peer translator.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	Use this command to clear entries from the translation table before they time out.
------------------	--

Examples	The following example shows the SNAT entries before and after using the clear ip snat sessions command:
----------	--

```
Router# show ip snat distributed

SNAT:Mode PRIMARY
      :State READY
      :Local Address 192.168.123.2
      :Local NAT id 100
      :Peer Address 192.168.123.3
      :Peer NAT id 200
      :Mapping List 10

Router# clear ip snat sessions *
Closing TCP session to peer:192.168.123.3
Router# show ip snat distributed
```

clear ip snat translation distributed

To clear dynamic Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation distributed** command in EXEC mode.

clear ip snat translation distributed *

Syntax Description	*	Removes all dynamic SNAT entries.
---------------------------	---	-----------------------------------

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	Use this command to clear entries from the translation table before they time out.
-------------------------	--

Examples	The following example clears all dynamic SNAT translations from the translation table:
-----------------	--

```
Router# clear ip snat translations distributed *
```

clear ip snat translation peer

To clear peer Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation peer** command in EXEC mode.

clear ip snat translation peer *ip-address-peer* [**refresh**]

Syntax Description		
	<i>ip-address-peer</i>	IP address of the peer translator.
	refresh	(Optional) Provides a fresh dump of the NAT table from the peer.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use this command to clear peer entries from the translation table before they time out.

Examples The following example shows the SNAT entries before and after the peer entry is cleared:

```
Router# show ip snat peer

Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.25.20      192.168.122.20   ---               ---
tcp 192.168.25.20:33528 192.168.122.20:33528 192.168.24.2:21 192.168.24.2:21

Router# clear ip snat translation peer 192.168.122.20
```

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear ip wccp** command in EXEC mode.

```
clear ip wccp {web-cache | service-number}
```

Syntax Description	web-cache	Directs the router to remove statistics for the web cache service.
	<i>service-number</i>	Directs the router to remove statistics for a specified cache service. The number can be from 0 to 99.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.1 CA	This command was introduced for Cisco 7200 and 7500 platforms.
	11.2 P	Support for this command was added to a variety of Cisco platforms.
	12.0(3)T	This command was expanded to be explicit about service using the web-cache keyword and the <i>service-number</i> argument.

Usage Guidelines Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics. If Cisco Cache Engines are used in your service group, the reverse proxy service is indicated by a value of 99.

Examples In the following example, all statistics associated with the web cache service are removed:

```
Router# clear ip wccp web-cache
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a cache engine service group.
	show ip wccp	Displays global statistics related to the WCCP.

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in privileged 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:

```
Router# clear tcp statistics
```

Related Commands	Command	Description
	show tcp statistics	Displays TCP statistics.

clear time-range ipc

To clear the time-range interprocess communications (IPC) message statistics and counters between the Route Processor and the line card, use the **clear time-range ipc** command in privileged EXEC mode.

clear time-range ipc

Syntax Description This command has no argument or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Examples The following example clears the time-range IPC statistics and counters:

```
Router# clear time-range ipc
```

Related Commands	Command	Description
	debug time-range ipc	Enables debugging output for monitoring the time-range IPC messages between the Route Processor and the line card.
	show time-range ipc	Displays the statistics about the time-range IPC messages between the Route Processor and line card.

client

To define which clients are allowed to use the virtual server, use the **client** SLB virtual server configuration command. You can use more than one client command to define more than one client. To remove a client definition from the IOS SLB configuration, use the **no** form of this command.

client *ip-address network-mask*

no client *ip-address network-mask*

Syntax Description

<i>ip-address</i>	Client IP address. The default is 0.0.0.0 (all clients).
<i>network-mask</i>	Client IP network mask. The default is 0.0.0.0 (all subnetworks).

Defaults

The default IP address is 0.0.0.0 (all clients).

The default network mask is 0.0.0.0 (all subnetworks).

Taken together, the default is **client 0.0.0.0 0.0.0.0** (allows all clients on all subnetworks to use the virtual server).

Command Modes

SLB virtual server configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The *network-mask* value is applied to the source IP address of incoming connections. The result must match the *ip-address* value for the client to be allowed to use the virtual server.

Examples

The following example allows only clients from 10.4.4.x access to the virtual server:

```
ip slb vserver PUBLIC_HTTP
  client 10.4.4.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** command in DHCP pool configuration mode. To delete the client identifier, use the **no** form of this command.

client-identifier *unique-identifier*

no client-identifier

Syntax Description	<i>unique-identifier</i>	The distinct identification of the client in dotted-hexadecimal notation, for example, 01b7.0813.8811.66.
---------------------------	--------------------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	DHCP pool configuration
----------------------	-------------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines

This command is valid for manual bindings only. DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address b708.1388.f166 is 01b7.0813.88f1.66, where 01 represents the Ethernet media type. For a list of media type codes, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, *Assigned Numbers*.

You can determine the client identifier by using the **debug ip dhcp server packet** command.

Examples

The following example specifies the client identifier for MAC address 01b7.0813.8811.66 in dotted hexadecimal notation:

```
client-identifier 01b7.0813.8811.66
```

Related Commands	Command	Description
	hardware-address	Specifies the hardware address of a BOOTP client.
	host	Specifies the IP address and network mask for a manual binding to a DHCP client.
	ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

client-name

To specify the name of a DHCP client, use the **client-name** command in DHCP pool configuration mode. To remove the client name, use the **no** form of this command.

client-name *name*

no client-name

Syntax Description	<i>name</i>	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name mars should not be specified as mars.cisco.com .
---------------------------	-------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	DHCP pool configuration
----------------------	-------------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines	The client name should not include the domain name.
-------------------------	---

Examples	The following example specifies a string client1 that will be the name of the client: <pre>client-name client1</pre>
-----------------	---

Related Commands	Command	Description
	host	Specifies the IP address and network mask for a manual binding to a DHCP client.
	ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

crypto ipsec

To enable security parameter index (SPI) matching between two Virtual Private Network (VPN) devices, use the **crypto ipsec** command on both devices in global configuration mode. To disable SPI matching, use the **no** form of this command.

crypto ipsec spi-matching

no crypto ipsec spi-matching

Syntax Description	spi-matching	Enables SPI matching on both endpoints.
Defaults	SPI matching in IPsec is not enabled by default.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(15)T	This command was introduced.
Usage Guidelines	The generation of SPIs that are predictable and symmetric is enabled. SPI matching should be used in conjunction with Network Address Translation (NAT) devices when multiple ESP connections across a NAT device is desired.	
Examples	The following example enables SPI matching on the endpoint routers: <pre>crypto ipsec spi-matching</pre>	
Related Commands	Command	Description
	clear ip nat translation	Clears dynamic NAT translations from the translation table.
	ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
	ip nat inside destination	Enables NAT of the inside destination address.
	ip nat inside source	Enables NAT of the inside source address.
	ip nat outside source	Enables NAT of the outside source address.
	show ip nat statistics	Displays NAT statistics.
	show ip nat translations	Displays active NAT translations.