

IP Commands

This chapter describes the function and displays the syntax of IP commands. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[no] access-class *access-list-number* {**in** | **out**}

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-list-number Number of an access list. This is a decimal number from 1 through 99.

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.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-mask*]
no access-list *access-list-number*

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-number Number of an access list. This is a decimal number from 1 through 99.

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. It is a 32-bit quantity in four-part dotted-decimal format.

source-mask (Optional) Mask to be applied to *source*. It is a 32-bit quantity in four-art dotted-decimal format. Place ones in the bit positions you want to mask.

access-list *access-list-number* { **deny** | **permit** } *protocol source source-mask destination destination-mask [operator operand]*

access-list *access-list-number* { **deny** | **permit** } **tcp** *source source-mask destination destination-mask [established]*

no access-list *access-list-number*

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-number Number of an access list. This is a decimal number from 100 through 199.

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 **ip**, **tcp**, **udp**, **icmp**, **igmp**, **gre**, or **igrp** or an integer in the range 0 through 255 representing an IP protocol number. To match any Internet protocol, including TCP, UDP, and ICMP, use the keyword **ip**.

source Number of the network or host from which the packet is being sent. It is a 32-bit quantity in four-part dotted-decimal format.

<i>source-mask</i>	Mask to be applied to <i>source</i> . It is a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to mask.
<i>destination</i>	Number of the network or host to which the packet is being sent. It is a 32-bit quantity in four-part dotted-decimal format.
<i>destination-mask</i>	Mask to be applied to <i>destination</i> . It is a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to mask.
<i>operator</i>	(Optional) Compares destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), and neq (not equal). Note that the ip and icmp protocol keywords do not allow port distinctions.
<i>operand</i>	(Optional) Decimal destination port to compare. Note that the ip and icmp protocol keywords do not allow port distinctions.
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.

[no] arp *ip-address hardware-address type* [**alias**]

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

<i>ip-address</i>	IP address in four-part dotted-decimal format corresponding to the local data link address.
<i>hardware-address</i>	Local data link address (a 48-bit address).
<i>type</i>	Encapsulation description. For Ethernet interfaces, this is typically the arpa keyword. For FDDI and Token Ring interfaces, this is always snap .
alias	(Optional) Indicates that the router should respond to ARP requests as if it were the owner of the specified address.

[no] arp {**arpa** | **probe** | **snap**}

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

arpa	Standard Ethernet-style ARP (RFC 826); the default
probe	HP Probe protocol for IEEE-802.3 networks
snap	ARP packets conforming to RFC 1042

[no] arp timeout *seconds*

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

<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.
----------------	--

clear arp-cache

To delete all dynamic entries from the ARP cache, to clear the fast-switching cache, and to clear the IP route cache, use the **clear arp-cache** EXEC command.

clear host {*name* | *}

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

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

clear ip accounting [**checkpoint**]

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

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

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

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

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

clear ip sse

To have the route processor recompute the SSE program for IP on the Cisco 7000 series, use the **clear ip sse** EXEC command.

clear sse

To reinitialize the route processor on the Cisco 7000 series, use the **clear sse** EXEC command.

[no] dnsix-dmdp retries *count*

To set the retransmit count used by the DNSIX Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** global configuration command. To restore the default number of retries, use the **no** form of this command.

count Number of times DMDP will retransmit a message. It can be a decimal integer from 0 through 200. The default is 4 retries, or until acknowledged.

[no] dnsix-nat authorized-redirection *ip-address*

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** global configuration command. To delete an address, use the **no** form of this command.

ip-address IP address of the host from which redirection requests are permitted

[no] dnsix-nat primary *ip-address*

To specify the IP address of the host to which DNSIX audit messages are sent, use the **dnsix-nat primary** global configuration command. To delete an entry, use the **no** form of this command.

ip-address IP address for the primary collection center

[no] dnsix-nat secondary *ip-address*

To specify an alternate IP address for the host to which DNSIX audit messages are sent, use the **dnsix-nat secondary** global configuration command. To delete an entry, use the **no** form of this command.

ip-address IP address for the secondary collection center

[no] dnsix-nat source *ip-address*

To start the audit-writing module and to define audit trail source address, use the **dnsix-nat source** global configuration command. To disable the DNSIX audit trail writing module, use the **no** form of this command.

ip-address Source IP address for DNSIX audit messages

[no] dnsix-nat transmit-count *count*

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** global configuration command. To revert to the default audit message count, use the **no** form of this command.

count Number of audit messages to buffer before transmitting to the server. Integer from 1 through 200. The default is 1.

[no] ip access-group *access-list-number* {**in** | **out**}

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. If a keyword is not specified, **out** is the default.

access-list-number Number of an access lists. This is a decimal number from 1 through 199.

in Filters on inbound packets.

out Filters on outbound packets.

[no] ip accounting [access-violations]

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.

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

[no] ip accounting-list *ip-address mask*

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-address IP address in dotted-decimal format
mask IP mask

[no] ip accounting-threshold *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.

threshold Maximum number of entries (source and destination address pairs) that the router accumulates. The default is 512 entries.

ip accounting-transits *count*

no 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.

count Number of transit records to store in the IP accounting database. The default is 0.

[no] ip address *ip-address mask*

To set an IP address for an interface, use the **ip address** interface configuration command. To remove an IP address, use the **no** form of this command.

ip-address IP address
mask Mask for the associated IP subnet

[no] ip address *ip-address mask secondary*

To set multiple IP addresses for an interface, use the **ip address secondary** interface configuration command. To remove an address, use the **no** form of this command.

ip-address IP address
mask Mask for the associated IP subnet

[no] ip broadcast-address [*ip-address*]

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restore the default IP broadcast address, use the **no** form of this command.

ip-address (Optional) IP broadcast address for a network. The default address is 255.255.255.255 (all ones).

ip cache-invalidate-delay [*minimum maximum quiet threshold*]
no ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** global configuration command. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

minimum (Optional) Minimum time, in seconds, between invalidation request and actual invalidation. The default is 2 seconds.

- maximum* (Optional) Maximum time, in seconds, between invalidation request and actual invalidation. The default is 5 seconds.
- quiet* (Optional) Length of quiet period, in seconds, before invalidation.
- threshold* (Optional) Maximum number of invalidation requests considered to be quiet.

[no] ip default-gateway *ip-address*

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** global configuration command. To disable this function, use the **no** form of this command.

ip-address IP address of the router

[no] ip directed-broadcast [*access-list-number*]

To enable the translation of directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

access-list-number (Optional) Number of the access list. If specified, a broadcast must pass the access list to be forwarded. If not specified, all broadcasts are forwarded.

[no] ip domain-list *name*

To define a list of default domain names to complete unqualified host names, use the **ip domain-list** global configuration command. To delete a name from a list, use the **no** form of this command.

name Domain name. Do not include the initial period that separates an unqualified name from the domain name.

[no] ip domain-lookup

To enable the IP Domain Name System-based host name-to-address translation, use the **ip domain-lookup** global configuration command. To disable the Domain Name System, use the **no** form of this command.

[no] ip domain-lookup nsap

To allow Domain Name System (DNS) queries for CLNS addresses, use the **ip domain-lookup nsap** global configuration command. To disable this feature, use the **no** form of this command.

ip domain-name *name*

no ip domain-name

To define a default domain name that the router uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain-name** global configuration command. To disable use of the Domain Name System, use the **no** form of this command.

name Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.

[no] ip forward-protocol {udp [*port*] | nd | sdns}

To specify which protocols and ports the router forwards, use the **ip forward-protocol** global configuration command. To remove a protocol or port, use the **no** form of this command.

udp Forward User Datagram Protocol (UDP) datagrams.

port (Optional) Destination port that controls which UDP services are forwarded.

nd Forward Network Disk (ND) datagrams. This protocol is used by older diskless SUN workstations.

sdns Network Security Protocol.

[no] ip forward-protocol spanning-tree

To permit IP broadcasts to be flooded throughout the internetwork in a controlled fashion, use the **ip forward-protocol spanning-tree** global configuration command. To disable the flooding of IP broadcasts, use the **no** form of this command.

[no] ip forward-protocol turbo-flood

To speed up flooding of User Datagram Protocol (UDP) datagrams using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** global configuration command. To disable this feature, use the **no** form of this command.

[no] ip gdp gdp

To configure the router discovery feature using the Cisco Gateway Discovery Protocol (GDP) routing protocol, use the **ip gdp gdp** interface configuration command. To disable this feature, use the **no** form of this command.

[no] ip gdp igrp

To configure the router discovery feature using the Cisco Interior Gateway Routing Protocol (IGRP), use the **ip gdp igrp** interface configuration command. To disable this feature, use the **no** form of this command.

[no] ip gdp irdp

To configure the router discovery feature using the ICMP Router Discovery Protocol (IRDP), use the **ip gdp irdp** interface configuration command. To disable this feature, use the **no** form of this command.

[no] ip gdp rip

To configure the router discovery feature using the Routing Information Protocol (RIP), use the **ip gdp rip** interface configuration command. To disable this feature, use the **no** form of this command.

[no] ip helper-address *address*

To have the router forward User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ip helper-address** interface configuration command. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

address Destination broadcast or host address to be used when forwarding UDP broadcasts. You can have more than one helper address per interface.

ip host *name* [*tcp-port-number*] *address1* [*address2...address8*]

no ip host *name* *address*

To define a static host name-to-address mapping in the host cache, use the **ip host** global configuration command. To remove the name-to-address mapping, use the **no** form of this command.

name Name of the host. The first character can be either a letter or a number, but if you use a number, the operations you can perform are limited.

tcp-port-number (Optional) TCP port number to connect to when using the defined host name in conjunction with an EXEC connect or telnet command. The default is Telnet (port 23).

address Associated IP address. You can bind up to eight addresses to a host name.

[no] ip hp-host *hostname ip-address*

To enter into the host table the host name of an HP host to be used for HP Probe Proxy service, use the **ip hp-host** global configuration command. To remove a host name, use the **no** form of this command.

hostname Name of the host
ip-address IP address of the host

[no] ip mask-reply

To have the router to 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 mtu *bytes*
no 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.

bytes MTU in bytes. The minimum is 128 bytes; the maximum depends on the interface medium.

[no] ip name-server *server-address1* [[*server-address2*]...
server-address6]

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** global configuration command. To remove the addresses specified, use the **no** form of this command.

server-address1...6 IP addresses of up to six name servers

[no] ip probe proxy

To enable the HP Probe Proxy support, which allows a router to respond to HP Probe Proxy Name requests, use the **ip probe proxy** interface configuration command. To disable HP Probe Proxy, use the **no** form of this command.

[no] ip proxy-arp

To enable proxy ARP on an interface, use the **ip proxy-arp** interface configuration command. To disable proxy ARP on the interface, use the **no** form of this command.

[no] ip redirects

To enable the sending of redirect messages if the router 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.

[no] ip route-cache [cbus]

[no] ip route-cache same-interface

[no] ip route-cache sse

To control the use of a high-speed switching cache for IP routing as well as the use of autonomous switching, use the **ip route-cache** interface configuration command. To disable fast switching and autonomous switching, use the **no** form of this command.

cbus (Optional) Enables both autonomous switching and fast switching. By default, autonomous switching is disabled. By default, fast switching may be enabled or disabled, depending on the interface and medium.

same-interface Enables fast switching packets back out the interface on which they arrived. By default, fast switching may be enabled or disabled, depending on the interface and medium.

sse Enables SSE fast switching on the SSP board on the Cisco 7000 series. By default, SSE switching is disabled.

[no] ip routing

To enable IP routing on the router, use the **ip routing** global configuration command. To disable IP routing on the router, use the **no** form of this command.

[no] ip security add

To add a basic security option to all outgoing packets, use the **ip security add** interface configuration command. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

[no] ip security aeso *source compartment-bits*

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command. To disable AESO on an interface, use the **no** form of this command.

source Extended Security Option (ESO) source.
This can be an integer from 0 through 255.

compartment-bits Compartment bits in hexadecimal.

[no] ip security dedicated *level authority [authority...]*

To set the level of classification and authority on the interface, use the **ip security dedicated** interface configuration command. To reset the interface to the default classification and authorities, use the **no** form of this command.

level Degree of sensitivity of information. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.

authority Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

[no] ip security eso-info *source compartment-size default-bit*

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** global configuration command. To return to the default settings, use the **no** form of this command.

<i>source</i>	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 through 255.
<i>compartment-size</i>	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 through 16.
<i>default-bit</i>	Default bit value for any unsent compartment bits.

[no] ip security eso-max *source compartment-bits*

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** interface configuration command. To return to the default, use the **no** form of this command.

<i>source</i>	Extended Security Option (ESO) source. An integer from 1 through 255.
<i>compartment-bits</i>	Compartment bits in hexadecimal.

[no] ip security eso-min *source compartment-bits*

To configure the minimum sensitivity for an interface, use the **ip security eso-min** interface configuration command. To return to the default, use the **no** form of this command.

<i>source</i>	Extended Security Option (ESO) source. An integer from 1 through 255.
<i>compartment-bits</i>	Compartment bits in hexadecimal.

[no] ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** interface configuration command. To restore the default, use the **no** form of this command.

[no] ip security first

To prioritize the presence of security options on a packet, use the **ip security first** interface configuration command. To disable this function, use the **no** form of this command.

[no] ip security ignore-authorities

To have the router ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** interface configuration command. To disable this function, use the **no** form of this command.

[no] ip security implicit-labelling [*level authority [authority...]*]

To force the router to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** interface configuration command. To disable this function, use the **no** form of this command.

- level* (Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.
- authority* (Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

ip security multilevel *level1 [authority1...] to level2 authority2 [authority2...]*

no ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** interface configuration command. To disable this function, use the **no** form of this command.

- level1* Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.
- authority1* (Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

to	Separates the range of classifications and authorities.
<i>level2</i>	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. The level keywords are listed in the IPSO level keywords table in the <i>Router Products Command Reference</i> publication.
<i>authority2</i>	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. The authority keywords are listed in IPSO authority keywords table in the <i>Router Products Command Reference</i> publication.

[no] ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** interface configuration command. To disable this feature, use the **no** form of this command.

[no] ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** interface configuration command. To disable this function, use the **no** form of this command.

[no] ip source-route

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

[no] ip subnet-zero

To enable the use of subnet zero for interface addresses and routing updates, use the **ip subnet-zero** global configuration command. To restore the default, use the **no** form of this command.

[no] ip tcp compression-connections *number*

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.

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

[no] ip tcp header-compression [passive]

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

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 router compresses all traffic.

[no] ip tcp synwait-time *seconds*

To set a period of time the router 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.

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

[no] ip unnumbered *interface-name*

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** interface configuration command. To disable the IP processing on the interface, use the **no** form of this command.

interface-name Name of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

[no] ip unreachable

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

ping [*protocol*] {*host* | *address*}

To check host reachability and network connectivity, use the **ping** (IP packet internet groper function) EXEC command.

protocol (Optional) Protocol keyword. The default is IP.
host Host name of system to ping.
address IP address of system to ping.

show access-lists

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

show arp

To display the entries in the ARP table for the router, use the show **arp** privileged EXEC command.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix** privileged EXEC command.

show hosts

To display 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, use the **show hosts** EXEC command.

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

To display the active accounting or checkpointed database, use the **show ip accounting** privileged EXEC command.

checkpoint	(Optional) Displays the checkpointed database.
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.

show ip aliases

To display the router's IP addresses mapped to TCP ports (aliases) and SLIP addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where SLIP addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** EXEC command.

show ip interface [*type number*]

To display the usability status of interfaces, use the **show ip interface** EXEC command.

type (Optional) Interface type
number (Optional) Interface number

show ip masks *address*

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** EXEC command.

address Network address for which a mask is required

show ip redirects

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

show ip route [*address* [*mask*] | *protocol*]

To display the entries in the routing table, use the **show ip route** EXEC command.

<i>address</i>	(Optional) Address about which routing information should be displayed.
<i>mask</i>	(Optional) Argument for a subnet mask.
<i>protocol</i>	(Optional) Argument for a particular routing protocol, or static or connected .

show ip route summary

To display summary information about entries in the routing table, use the **show ip route summary** EXEC command.

show ip tcp header-compression

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

show ip traffic

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

show sse summary

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** EXEC command.

show standby

To display standby protocol information, use the **show standby** EXEC command.

[no] standby authentication *string*

To configure an authentication string, use the **standby authentication** interface configuration command. To delete an authentication string, use the **no** form of this command.

string Authentication string. It can be up to eight characters in length. The default string is **cisco**.

[no] standby group *number*

To specify the number of the Hot Standby group in which the router will participate, use the **standby group** interface configuration command. To use the default group number, use the **no** form of this command.

number The group number. It is an integer between 0 and 255. The default is group number 0.

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

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

ip-address (Optional) IP address of the Hot Standby Router interface

[no] standby preempt

To indicate that, when the local router is configured with a priority higher than the current designated router, the local router should attempt to assume control as the designated router, use the **standby preempt** interface configuration command. To have the local router assume control as the designated router only if it receives information indicating that there is no router currently in the active state (acting as the designated router), use the **no** form of this command.

[no] standby priority *number*

To prioritize a potential Hot Standby router, use the **standby priority** interface configuration command. To restore the priority to the default, use the **no** form of this command.

number Priority value. It is an integer from 0 through 255.
The default is 100.

[no] standby timers *hellotime holdtime*

To configure the time between hellos and the time before other routers declare the active 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.

hellotime Hello interval in seconds. This is an integer from 1 through 255. The default is 1 second.

holdtime Time in seconds before the active or standby router is declared to be down. This is an integer from 1 through 255. The default is 3 seconds.

trace ip *destination*

To discover the routes the router's packets follow when traveling to their destination, use the trace user EXEC command.

destination (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

trace [*destination*]

To discover the routes the router's packets follow when traveling to their destination, use the **trace** privileged EXEC command.

destination (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

transmit-interface *interface-name*
no 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.

interface-name Transmit interface to be linked with the (current) receive-only interface