IP Commands

This section 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**}

Use the **access-class** line configuration command to restrict incoming and outgoing connections between a particular virtual terminal line (into a Cisco device) and the addresses in an access list. The **no** form of this command removes access restrictions on the line for the specified connections.

access-list-number	Integer from 1 through 99 that identifies a specific access list of Internet addresses.
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* {**permit** | **deny**} *source* [*source-mask*]
no access-list *access-list-number*

Use the **access-list** global configuration command to create or remove a standard access list and control access to it. Use the **no** form of this command to delete the entire access list.

access-list-number	Integer from 1 through 99 that you assign to identify one or more permit/deny conditions as an access list. Access list 0 (zero) is predefined; it permits any address and is the default access list for all interfaces.
permit	Permits access for matching conditions.
deny	Denies access to matching conditions.
source	Compares the source address being tested to this value. It is a 32-bit quantity written in dotted-decimal format.
source-mask	(Optional) 32-bit quantity written in dotted-decimal format. Address bits corresponding to wildcard mask bits set to 1 are ignored in comparisons; address bits corresponding to wildcard mask bits set to zero are used in comparisons.

access-list *access-list-number* {**permit** | **deny**} *protocol source source-mask destination destination-mask* [*operator operand*] [**established**]
no access-list *access-list-number*

Use the extended access-list global configuration command to create or remove an extended access list. Use the **no** form of this command to delete the entire extended access list. An extended access list defaults to an implicit deny statement for everything that has not been permitted.

access-list-number	Integer from 100 through 199 that you assign to identify one or more extended permit/deny conditions as an extended access list.

permit	Permits access to matching conditions.
deny	Denies access to matching conditions.
protocol	One of the following protocols: **ip**, **tcp**, **udp**, **icmp**, **igmp**, **gre**, or **igrp** or an integer in the range of 0 through 255 representing an IP protocol number. Use the keyword **ip** to match any Internet protocol, including TCP, UDP, and ICMP.
source	Internet source address in dotted-decimal format.
source-mask	Mask of source address bits in dotted-decimal format. The *source* and *source-mask* arguments are used to match the source address of a packet.
destination	Internet destination address in dotted-decimal format.
destination-mask	Mask of destination address bits in dotted-decimal format. The destination and destination mask arguments are used to match the destination address of a packet.
operator	(Optional) Compares destination ports. Note that the **ip** and **icmp** protocol keywords do not allow port distinctions. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), and **neq** (not equal).
operand	(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: to indicate 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**]

Use the **arp** global configuration command to install a permanent entry in the ARP cache. The router uses this entry to translate 32-bit Internet Protocol addresses into 48-bit hardware addresses. Use the **no** form of this command to remove the specified entry from the ARP cache. By default, no entries are permanently installed in the ARP cache.

ip-address	Internet address in dotted-decimal format corresponding to the local data link address.
hardware-address	Local data link address (a 48-bit address).
type	Encapsulation description. This is typically the **arpa** keyword for Ethernet and is always **snap** for FDDI and Token Ring interfaces.
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**}

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

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*

Use the **arp timeout** interface configuration command to control the number of seconds an ARP cache entry will stay in the cache. Use the **no** form of this command to restore the default value.

seconds	Value used to age an ARP cache entry related to that interface. A value of 0 (zero) seconds sets no timeout; then the cache entries are never cleared. The default is 14400 seconds (4 hours).

clear arp-cache

Use the **clear arp-cache** privileged EXEC command to remove all dynamic entries from the ARP cache, to clear the fast-switching cache, and to clear the IP route cache.

clear host {*name* | *****}

Use the **clear host** privileged EXEC command to remove one or all entries from the host name-and-address cache.

name	Particular host entry to remove.
*****	Removes all entries.

clear ip accounting [**checkpoint**]

Use the **clear ip accounting** privileged EXEC command to clear the active database when IP accounting is enabled. Use the **clear ip accounting checkpoint** command to clear the checkpointed database when IP accounting is enabled.

checkpoint	(Optional) Clears the checkpointed database.

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

Use the **clear ip route** privileged EXEC command to remove one or more routes from the IP routing table. By default, all entries are removed.

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

clear ip sse

Use the **clear ip sse** privileged EXEC command to cause the route processor to recompute the program for IP on the Cisco 7000 series.

[**no**] **dnsix-dmdp retries** *count*

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

count	Number of times DMDP will retransmit a message. An integer from 0 through 200. The default is 4 retries.

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

Use the dnsix-nat authorized-redirection global configuration command 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 **no** form of this command to delete the entry.

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

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

Use the **dnsix-nat primary** global configuration command to specify the IP address of the host to which DNSIX audit messages are sent. Use the **no** form of this command to delete the entry. By default, messages are not sent.

ip-address	IP address for the primary collection center

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

Use the **dnsix-nat secondary** global configuration command to specify an alternate IP address for the host to which DNSIX audit messages are sent. Use the **no dnsix-nat secondary** command to delete the entry. By default, no alternate IP address is known.

ip-address	IP address for the secondary collection center

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

Use the **dnsix-nat source** global configuration command to start the audit-writing module and to define audit trail source address. Use the **no** form of this command to disable the DNSIX audit trail writing module. By default, the module is disabled.

ip-address	Source IP address for DNSIX audit messages

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

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

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**}

Use the **ip access-group** interface configuration command to control access to an interface. Use the **no** form of this command to remove the specified access group. If a keyword is not specified, **out** is the default.

access-list-number	Access list number from 1 through 199.
in	Filters on inbound packets.
out	Filters on outbound packets.

[**no**] **ip accounting**

Use the **ip accounting** interface configuration command to enable IP accounting on an interface. Use the **no ip accounting** command to disable IP accounting. By default, IP accounting is disabled.

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

Use the **ip accounting-list** global configuration command to specify a set of filters to control the hosts for which IP accounting information is kept. Use the **no** form of this command with the appropriate argument to remove this function. By default, no filters are defined.

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

[**no**] **ip accounting-threshold** *threshold*

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

threshold	Maximum number of entries (source and destination address pairs) that the router accumulates, preventing IP accounting from possibly consuming all available free memory. The default is 512 entries.

ip accounting-transits *count*
no ip accounting-transits

Use the **ip accounting-transits** global configuration command to control the number of transit records that will be stored in the IP accounting database. Use the **no** form of this command to remove this function, resetting the value to the default.

count	Number of transit records that will be stored in the IP accounting database. The default is 0.

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

Use the **ip address** interface configuration command to set an IP address for an interface. Use the **no** form of this command to remove the specified address.

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

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

Use the **ip address secondary** interface configuration command to set multiple IP addresses for an interface. Use the **no** form of this command to remove the specified addresses.

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

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

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

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

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

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*

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

ip-address	IP address of the router

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

Use the **ip directed-broadcast** interface configuration command to enable directed broadcast-to-physical broadcast translation on an interface. Use the **no** form of this command to disable directed broadcast-to-physical broadcast translation on an interface.

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 will be forwarded.

[**no**] **ip domain-list** *name*

Use the **ip domain-list** global configuration command to define a list of default domain names to complete unqualified host names. Use the **no** form of this command with the appropriate argument to delete a name from the list.

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

[**no**] **ip domain-lookup**

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

[**no**] **ip domain-lookup nsap**

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

ip domain-name *name*
no ip domain-name

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

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** | **snds**}

Use the **ip forward-protocol** global configuration command to specify which protocols and ports the router will forward. Use the **no** form of this command (with the appropriate keyword and argument) to remove the protocol/port. See this command in the *Router Products Command Reference* publication for a list of datagrams forwarded by default.

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.
snds	Network Security Protocol.

[**no**] **ip forward-protocol spanning-tree**

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

[**no**] **ip forward-protocol turbo-flood**

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

[**no**] **ip gdp gdp**

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

[**no**] **ip gdp igrp**

Use the **ip gdp igrp** interface configuration command to configure the router discovery feature using the Cisco Interior Gateway Routing Protocol (IGRP) routing protocol. Use the **no** form of this command to disable this feature.

[**no**] **ip gdp irdp**

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

[**no**] **ip gdp rip**

Use the **ip gdp rip** interface configuration command to configure the router discovery feature using the RIP routing protocol. Use the **no** form of this command to disable this feature.

[**no**] **ip helper-address** *address*

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

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*

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

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—Telnet by default (port 23).
address	Associated IP address. Up to eight addresses can be bound to a host name.

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

Use the **ip hp-host** global configuration command to enter the host name of an HP host to be used for HP Probe Proxy service into the host table. Use the **no** form of this command with the appropriate arguments to remove the host name.

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

[**no**] **ip mask-reply**

Use the **ip mask-reply** interface configuration command to tell the router to respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP Mask Reply messages. Use the **no** form of this command to disable this function.

ip mtu *bytes*
no ip mtu

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

bytes	IP MTU in bytes. Minimum is 128 bytes; maximum depends on interface medium type.

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

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

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

[**no**] **ip probe proxy**

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

[**no**] **ip proxy-arp**

Use the **ip proxy-arp** interface configuration command to enable proxy ARP on an interface. Use the **no** form of this command to disable proxy ARP on the interface.

[**no**] **ip redirects**

Use the **ip redirects** interface configuration command 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 **no** form of this command to disable the sending of redirect messages.

[**no**] **ip route-cache** [**cbus**]
[**no**] **ip route-cache same-interface**
[**no**] **ip route-cache sse**

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

cbus	(Optional) Enables both autonomous switching and fast switching. By default, IP autonomous switching is disabled; fast switching varies by interface and media.
same-interface	Enables fast switching packets back out the interface on which they arrived. Fast switching varies by interface and media.
sse	Enables SSE fast switching on the SSP board on the Cisco 7000 series. By default, SSE switching of IP is disabled.

[**no**] **ip routing**

Use the **ip routing** global configuration command to enable IP routing. Use the **no** form of this command to disable IP routing for the router.

[**no**] **ip security add**

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

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

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

source	Extended Security Option (ESO) source. An integer from 0 through 255.
compartment-bits	Compartment bits in hex.

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

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

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

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

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

source	Hex or decimal value representing the extended IPSO source. An integer from 0 through 255.

compartment-size	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. An integer from 1 through 16.
default-bit	Default bit value for any unsent compartment bits.

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

Use the **ip security eso-max** interface configuration command to specify the maximum sensitivity level for an interface. Use the **no** form of this command to revert to the default.

source	Extended Security Option (ESO) source. An integer from 1 through 255.
compartment-bits	Compartment bits in hex.

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

Use the **ip security eso-min** interface configuration command to configure the minimum sensitivity for an interface. Use the **no** form of this command to revert to the default.

source	Extended Security Option (ESO) source. An integer from 1 through 255.
compartment-bits	Compartment bits in hex.

[**no**] **ip security extended-allowed**

Use the **ip security extended-allowed** interface configuration command to accept packets on an interface that has an extended security option present. Packets containing extended security options are rejected. Use the **no** form of this command to restore the default.

[**no**] **ip security first**

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

[**no**] **ip security ignore-authorities**

Use the **ip security ignore-authorities** interface configuration command to cause the router to ignore the authorities field of all incoming packets. Use the **no** form of this command to disable this function.

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

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

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 and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).
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 the IPSO authority keywords and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).

ip security multilevel *level1* [*authority1...*] **to** *level2 authority2* [*authority2...*]
no ip security multilevel

Use the **ip security multilevel** interface configuration command to set the interface to the requested range of classifications and authorities. All traffic entering or leaving the system must have a security option that falls within this range.

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 found in the IPSO level keywords and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).
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 the IPSO authority keywords and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).
to	Separates the range of classifications and authorities.
level2	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 found in the IPSO level keywords and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).
authority2	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 the IPSO authority keywords and bit patterns table in the *Router Products Command Reference* publication (see the **ip security dedicated** command).

[**no**] **ip security reserved-allowed**

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

[**no**] **ip security strip**

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

[**no**] **ip source-route**

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

[**no**] **ip subnet-zero**

Use the **ip subnet-zero** global configuration command to enable use of subnet zero for interface addresses and routing updates. Hence, it provides the ability to configure and route to subnet-zero subnets. Use the **no** form of this command to restore the default.

[**no**] **ip tcp compression-connections** *number*

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

number	Number of connections the cache will support; *number* can vary between 3 and 256, inclusive. The default is 16.

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

Use the **ip tcp header-compression** interface configuration command to enable TCP header compression. Use the **no** form of this command to disable compression.

passive	(Optional) Outgoing TCP packets are compressed 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*

Use the **ip tcp synwait-time** global configuration command to set a specified period of time the router will wait to attempt to establish a TCP connection before it times out. The **no** form of this command restores the default.

seconds	Number of seconds the router waits to attempt to establish a TCP connection. Use any value between 5 and 300 seconds. The default is 30 seconds.

[**no**] **ip unnumbered** *interface-name*

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

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

[**no**] **ip unreachables**

Use the **ip unreachables** interface configuration command to enable the generation of ICMP Unreachable messages on a specified interface. Use the **no** form of this command to disable this function.

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

Use the **ping** (IP packet internet groper function) privileged EXEC command to send ICMP *Echo* messages to check host reachability and network connectivity. If the router receives an ICMP *Echo* message, it sends an ICMP *Echo Reply* message to the source of the ICMP *Echo* message.

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

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

Use the **ping** (IP packet internet groper function) user EXEC command to send ICMP *Echo* messages to check host reachability and network connectivity. If the router receives an ICMP *Echo* message, it sends an ICMP *Echo Reply* message to the source of the ICMP *Echo* message.

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

show access-lists

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

show arp

Use the **show arp** privileged EXEC command to display the entries in the ARP table for the router.

show dnsix

Use the **show dnsix** privileged EXEC command to display state information and the current configuration of the DNSIX audit writing module.

show hosts

Use the **show hosts** EXEC command 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.

show ip accounting [**checkpoint**]

Use the **show ip accounting** privileged EXEC command to display the active accounting or checkpointed database.

checkpoint	(Optional) Indicates that the checkpointed database should be displayed.

show ip aliases

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

show ip arp

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

show ip cache

Use the **show ip cache** EXEC command to display the routing table cache used to fast switch Internet traffic.

show ip interface [*interface unit*]

Use the **show ip interface** EXEC command to display the usability status of interfaces.

interface unit	(Optional) Interface type and number.

show ip masks *address*

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

address	Network address for which a mask is required

show ip redirects

Use the **show ip redirects** EXEC command to display the address of a default gateway (router).

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

Use the **show ip route** EXEC command to display the current state of the routing table.

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

show ip route summary

Use the **show ip route summary** EXEC command to display the current state of the routing table.

show ip tcp header-compression

Use the **show ip tcp header-compression** EXEC command to display statistics on TCP header compression.

show ip traffic

Use the **show ip traffic** EXEC command to display IP protocol statistics.

show sse summary

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

show standby

Use the **show standby** EXEC command to display standby protocol information.

[**no**] **standby authentication** *string*

Use the **standby authentication** interface configuration command to configure an authentication string. Use the **no** form of this command to delete the authentication string.

string	Authentication string, up to eight characters long. The default string is "cisco."

[**no**] **standby group** *number*

Use the **standby group** interface configuration command to specify the number of the group in which the router will participate. Use the **no** form of this command to use the default group.

number	The group number. An integer between 0 and 255. The default is group number 0.

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

Use the **standby ip** interface configuration command to activate the hot standby protocol on the configured interface. Use the **no** form of this command to disable the standby function on an interface.

ip-address	(Optional) Interface hot standby IP address

[**no**] **standby preempt**

Use the **standby preempt** interface configuration command to indicate that, if 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 **no** form of this command to cause the local router to 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).

[**no**] **standby priority** *number*

Use the **standby priority** interface configuration command to prioritize a potential hot standby router. Use the **no** form of this command to restore the priority to the default.

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

[**no**] **standby timers** *hellotime holdtime*

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

hellotime	Hello interval in seconds. An integer between 1 and 255. The default is 1 second.
holdtime	Time in seconds before the active or standby router is declared to be down. An integer between 1 and 255. The default is 3 seconds.

trace [*destination*]

Use the **trace** privileged EXEC command to discover the routes the router's packets will actually take when traveling to their destination.

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 ip *destination*

Use the **trace ip** user EXEC command to discover the IP routes the router's packets will actually take when traveling to their destination.

destination	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

Use the **transmit-interface** interface configuration command to assign a transmit interface to a receive-only interface. This is used commonly with microwave Ethernet links. The **no** form of this command reverts both interfaces to normal duplex Ethernet interfaces.

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