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.

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 **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 through 255 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword **ip**. Some protocols allow further qualifiers described below.

source — Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

source-wildcard — Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

destination Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence* (Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the “Precedence Names” table in the *Router Products Command Reference* publication.

tos *tos* (Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Type of Service Names” table in the *Router Products Command Reference* publication.

icmp-type (Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code

(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

icmp-message

(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “ICMP Message Type Names” table in the *Router Products Command Reference* publication.

igmp-type

(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “IGMP Message Names” table in the *Router Products Command Reference* publication.

operator

(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).

If the operator is positioned after the *source* and *source-wildcard*, it must match the source port.

If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port.

The **range** operator requires two port numbers. All other operators require one port number.

port

(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names are listed in the “TCP Port Names” table in the *Router Products Command Reference* publication. TCP port names can only be used when filtering TCP.

UDP port names are listed in the section “UDP Port Names” table in the *Router Products Command Reference* publication. UDP port names can only be used when filtering UDP.

established (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

log (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)

The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
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. There are two alternative ways to specify the source:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

source-wildcard (Optional) Wildcard bits to be applied to the *source*. There are two alternative ways to specify the source wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]
no access-list *access-list-number*

access-list *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For ICMP, you can also use the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For IGMP, you can also use the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **tcp** *source*
source-wildcard [*operator port* [*port*]] *destination*
destination-wildcard [*operator port* [*port*]] [**established**]
[**precedence** *precedence*] [**tos** *tos*] [**log**]

For TCP, you can also use the the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **udp** *source*
source-wildcard [*operator port* [*port*]] *destination*
destination-wildcard [*operator port* [*port*]] [**precedence** *precedence*]
[**tos** *tos*] [**log**]

For UDP, you can also use the syntax shown above.

[**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.

ip-address IP address in four-part dotted-decimal format corresponding to the local data link address.

hardware-address Local data link address (a 48-bit address).

type 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.

seconds	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 access-list counters *access-list-number*

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

access-list-number	Access list number from 0 to 1199 for which to clear the counters.

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.

name	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 nhrp

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

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

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

network	Network or subnet address to remove.
mask	(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* [**secondary**]

To set a primary or secondary IP address for an interface, use the **ip address** interface configuration command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

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

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restored 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 classless**

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the router forward such packets to the best supernet route possible, use the **ip classless** global configuration command. To disable this feature, use the **no** form of this command.

[**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 when forwarding broadcast packets, 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. See the "Default" section in the *Router Products Command Reference* publication for a list of port numbers forwarded by default.
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	Secure Data Network Service.

[**no**] **ip forward-protocol any-local-broadcast**

To forward any broadcasts including local subnet broadcasts, use the **ip forward-protocol any-local-broadcast** global configuration command. To disable this type of forwarding, use the **no** form of this command.

[**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.

[**no**] **ip mobile arp** [**timers** *keepalive hold-time*] [**access-group** *access-list-number*]

To enable local-area mobility, use the **ip mobile arp** interface configuration command. To disable local-area mobility, use the **no** form of this command.

timers (Optional) Indicates that you are setting local-area mobility timers.

keepalive (Optional) Frequency, in seconds, at which the router sends unicast ARP messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 300 seconds (5 minutes).

hold-time (Optional) Hold time, in seconds. This is the length of time the router considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 900 seconds (15 minutes).

access-group (Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.

access-list-number (Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.

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	IP address of name server.
server-address2 ... *server-address6*	(Optional) IP addresses of additional name servers (a maximum of six name servers).

ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}
no ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format** line configuration command. To restore the default display format, use the **no** form of this command.

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted decimal notation (for example, 255.255.255.0). The default is dotted decimal notation.
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

ip nhrp authentication *string*
no ip nhrp authentication [*string*]

To configure the authentication string for an interface using Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** interface configuration command. To remove the authentication string, use the **no** form of this command.

string Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to 8 characters long.

ip nhrp holdtime *seconds-positive* [*seconds-negative*]
no ip nhrp holdtime [*seconds-positive* [*seconds-negative*]]

To change the number of seconds that NHRP nonbroadcast, multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime** interface configuration command. To restore the default value, use the **no** form of this command.

seconds-positive Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The default is 7200 seconds (2 hours).

seconds-negative (Optional) Time in seconds that NBMA addresses are advertised as valid in negative authoritative NHRP responses. The default is 7200 seconds (2 hours).

ip nhrp interest *access-list-number*
no ip nhrp interest [*access-list-number*]

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) Request, use the **ip nhrp interest** interface configuration command. To restore the default value, use the **no** form of this command.

access-list-number Standard or extended IP access list number in the range 1 through 199.

ip nhrp map *ip-address nbma-address*
no ip nhrp map *ip-address nbma-address*

To statically configure the IP-to-NBMA address mapping of IP destinations connected to a nonbroadcast, multiaccess (NBMA) network, use the **ip nhrp map** interface configuration command. To remove the static entry from NHRP cache, use the **no** form of this command.

ip-address IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.

nbma-address Nonbroadcast, multiaccess (NBMA) address which is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has an NSAP address, Ethernet has a MAC address, and SMDS has an E.164 address. This address is mapped to the IP address.

[**no**] **ip nhrp map multicast** *nbma-address*

To configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** interface configuration command. To remove the destinations, use the **no** form of this command.

nbma-address Nonbroadcast, multiaccess (NBMA) address which is directly reachable through the NBMA network. The address format varies depending on the medium you are using.

ip nhrp network-id *number*
no ip nhrp network-id [*number*]

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** interface configuration command. To disable NHRP on the interface, use the **no** form of this command.

number Globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295.

[**no**] **ip nhrp nhs** *nhs-address* [*net-address* [*netmask*]]

To specify the address of one or more NHRP Next Hop Servers, use the **ip nhrp nhs** interface configuration command. To remove the address, use the **no** form of this command.

nhs-address Address of the Next Hop Server being specified.

net-address (Optional) IP address of a network served by the Next Hop Server.

netmask (Optional) IP network mask to be associated with the *net* IP address. The *net* IP address is logically ANDed with the mask.

[**no**] **ip nhrp record**

To re-enable the use of forward record and reverse record options in NHRP Request and Reply packets, use the **ip nhrp record** interface configuration command. To suppress the use of such options, use the **no** form of this command.

ip nhrp responder *type number*
no ip nhrp responder [*type*] [*number*]

To designate which interface's primary IP address the Next Hop Server will use in NHRP Reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** interface configuration command. To remove the designation, use the **no** form of this command.

type	Interface type whose primary IP address is used when a Next Hop Server complies with a Responder Address option (for example, **serial**, **tunnel**).
number	Interface number whose primary IP address is used when a Next Hop Server complies with a Responder Address option.

[**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 Prove 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.

source Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 through 255.

compartment-size Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 through 16.

default-bit 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.

source Extended Security Option (ESO) source. An integer from 1 through 255.

compartment-bits 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.

source Extended Security Option (ESO) source. An integer from 1 through 255.

compartment-bits 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.

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 listed in the IPSO level keywords table in the *Router Products Command Reference* publication.

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 IPSO authority keywords table in the *Router Products Command Reference* 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 path-mtu-discovery**

To enable Path MTU Discovery for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** interface configuration command. To disable the feature, use the **no** form of this command.

[**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** *type number*

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.

type number Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

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

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

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 access-list [*access-list-number*]

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

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

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 [*prefix mask*] [*type number*]

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

prefix (Optional) Display only the entries in the cache that match the prefix and mask combination.

mask (Optional) Display only the entries in the cache that match the prefix and mask combination.

type (Optional) Display only the entries in the cache that match the interface type and number combination.

number (Optional) Display only the entries in the cache that match the interface type and number combination.

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 nhrp [**dynamic** | **static**] [*type number*]

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ip nhrp** EXEC command.

dynamic (Optional) Displays only the dynamic (learned) IP-to-NBMA address cache entries.

static (Optional) Displays only the static IP-to-NBMA address entries in the cache (configured through the **ip nhrp map** command).

type (Optional) Interface type about which to display the NHRP cache (for example, **atm**, **tunnel**).

number (Optional) Interface number about which to display the NHRP cache.

show ip nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ip nhrp traffic** EXEC command.

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.

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

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 Hot Standby Router Protocol information, use the **show standby** EXEC command.

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

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

group-number	(Optional) Group number on the interface to which this authentication string applies. The default number is 0.
string	Authentication string. It can be up to eight characters in length. The default string is **cisco**.

[**no**] **standby** [*group-number*] **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.

group-number (Optional) Group number on the interface for which the Hot Standby Router Protocol is being activated. The default number is 0.

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

[**no**] **standby** [*group-number*] **preempt**

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

group-number (Optional) Group number on the interface for which the Hot Standby preemptive feature is being activated. The default number is 0.

[**no**] **standby** [*group-number*] **priority** *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.

group-number (Optional) Group number on the interface to which the priority number applies. The default number is 0.

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

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

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

group-number (Optional) Group number on the interface to which the timers apply. The default is 0.

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.

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

To configure an interface so that the router's Hot Standby priority changes based on the availability of other interfaces, use the **standby track** interface configuration command. To remove the tracking, use the **no** form of this command.

group-number (Optional) Group number on the interface to which the tracking applies. The default number is 0.

type Interface type (combined with interface number) that will be tracked.

number Interface number (combined with interface type) that will be tracked.

interface-priority (Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.

term ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}
term no ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format** EXEC command. To restore the default display format, use the **no** form of this command.

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.55/24 indicates that the netmask is 24 bits.
decimal	Netmasks are displayed in dotted decimal notation (for example, 255.255.255.0).
hexadecimal	Netmasks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

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 *type number*
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.

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

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** [**multipoint**] | **nos**}
no tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To set to the default, use the **no** form of this command.

aurp	AppleTalk Update Routing Protocol (AURP).
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre ip	Generic route encapsulation (GRE) protocol over IP.
multipoint	(Optional) Enables a GRE tunnel to be used in a multipoint fashion. Can be used with the **gre ip** keyword only, and requires the use of the **tunnel key** command.
nos	KA9Q/NOS compatible IP over IP.