



IP Addressing Commands

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. IP handles addressing, fragmentation, reassembly, and protocol demultiplexing. It is the foundation on which all other Internet protocols, collectively referred to as the *Internet Protocol suite*, are built. IP is a network-layer protocol that contains addressing information and some control information that allows data packets to be routed.

The Transmission Control Protocol (TCP) is built upon the IP layer. TCP is a connection-oriented protocol that specifies the format of data and acknowledgments used in the transfer of data. TCP also specifies the procedures that the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently because it handles all demultiplexing of the incoming traffic among the application programs.

Use the commands in this chapter to configure and monitor the addressing of IP networks. For IP addressing configuration information and examples, refer to the “Configuring IP Addressing” chapter of the *Network Protocols Configuration Guide, Part 1*.

arp (global)

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

arp *ip-address hardware-address type* [**alias**]

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

Syntax Description

<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 Fiber Distributed Data Interface (FDDI) and Token Ring interfaces, this is always snap .
alias	(Optional) Indicates that the Cisco IOS software should respond to ARP requests as if it were the owner of the specified address.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Because most hosts support dynamic resolution, you generally do not need to specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

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

```
arp 192.31.7.19 0800.0900.1834 arpa
```

Related Commands

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

arp (interface)

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

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

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

Syntax Description

arpa	Standard Ethernet-style ARP (RFC 826).
frame-relay	Enables ARP over a frame-relay encapsulated interface
probe	HP Probe protocol for IEEE-802.3 networks.
snap	ARP packets conforming to RFC 1042.
timeout	Set ARP cache timeout

Defaults

Standard Ethernet-style ARP

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Unlike most commands that take multiple arguments, arguments to the **arp** command are not mutually exclusive. Each command enables or disables a specific type of ARP. For example, if you enter the **arp arpa** command followed by the **arp probe** command, the Cisco IOS software would send three (two for **probe** and one for **arpa**) packets each time it needed to discover a Media Access Control (MAC) address.

The **arp probe** command allows the software to use the Probe protocol (in addition to ARP) whenever it attempts to resolve an IEEE-802.3 or Ethernet local data link address. The subset of Probe that performs address resolution is called Virtual Address Request and Reply. Using Probe, the software can communicate transparently with Hewlett-Packard IEEE-802.3 hosts that use this type of data encapsulation.



Note

Cisco's support for HP Probe proxy support changed as of Software Release 8.3(2) and subsequent software releases. The **no arp probe** command is now the default. All interfaces that will use Probe must now be explicitly configured for **arp probe**.

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

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

Examples

The following example enables probe services:

```
interface ethernet 0
  arp probe
```

Related Commands

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

arp timeout

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

arp timeout *seconds*

no arp timeout *seconds*

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

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

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

Command History	Release	Modification
	10.0	This command was introduced.

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

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

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

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

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

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 arp-cache

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

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

```
clear arp-cache
```

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

clear host

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The host name entries will not be removed from nonvolatile random-access memory (NVRAM), but will be cleared in running memory.

Examples

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

```
clear host *
```

Related Commands

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

clear ip nat translation

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

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

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

Syntax Description		
	*	Clears all dynamic translations.
	inside	Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
	<i>global-ip</i>	When used without the arguments <i>protocol</i> , <i>global-port</i> , and <i>local-port</i> , clears a simple translation that also contains the specified <i>local-ip</i> address. When used with the arguments <i>protocol</i> , <i>global-port</i> , and <i>local-port</i> , clears an extended translation.
	<i>local-ip</i>	(Optional) Clears an entry that contains this local IP address and the specified <i>global-ip</i> address.
	outside	Clears the outside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
	<i>protocol</i>	(Optional) Clears an entry that contains this protocol and the specified <i>global-ip</i> address, <i>local-ip</i> address, <i>global-port</i> , and <i>local-port</i> .
	<i>global-port</i>	(Optional) Clears an entry that contains this <i>global-port</i> and the specified <i>protocol</i> , <i>global-ip</i> address, <i>local-ip</i> address, and <i>local-port</i> .
	<i>local-port</i>	(Optional) Clears an entry that contains this <i>local-port</i> and the specified <i>protocol</i> , <i>global-ip</i> address, <i>local-ip</i> address, and <i>global-port</i> .

Command Modes	
	EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines

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

Examples

The following example shows the NAT entries before and after the UDP entry being cleared:

```
Router# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23

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

Router# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

Related Commands

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

clear ip nhrp

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

clear ip nhrp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced.

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

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

```
clear ip nhrp
```

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

clear ip route

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

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

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

Defaults All entries are removed.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

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

```
clear ip route 132.5.0.0
```

ip address

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* [**secondary**]

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

Syntax Description

<i>ip-address</i>	IP address.
<i>mask</i>	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.

Defaults

No IP address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional keyword **secondary** allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

**Note**

If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

**Note**

When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must do two things:

- Disable IP routing (specify **no ip routing**).
- Add the interface to a bridge group. (See the **bridge-group** command.)

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 131.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
ip address 131.108.1.27 255.255.255.0
ip address 192.31.7.17 255.255.255.0 secondary
ip address 192.31.8.17 255.255.255.0 secondary
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.

ip broadcast-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 broadcast-address [*ip-address*]

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

Syntax Description	<i>ip-address</i> (Optional) IP broadcast address for a network.
---------------------------	--

Defaults	Default address: 255.255.255.255 (all ones)
-----------------	---

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

Command History	Release	Modification
	10.0	This command was introduced.

Examples	<p>The following example specifies an IP broadcast address of 0.0.0.0:</p> <pre>ip broadcast-address 0.0.0.0</pre>
-----------------	--

ip cef traffic-statistics

To change the time interval that controls when NHRP will set up or tear down an SVC, use the **ip cef traffic-statistics** global configuration command. To restore the default values, use the **no** form of this command.

```
ip cef traffic-statistics [load-interval seconds] [update-rate seconds]
```

```
no ip cef traffic-statistics
```

Syntax Description

load-interval <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the ip nhrp trigger-svc command.) The load-interval range is 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate <i>seconds</i>	(Optional) Frequency that the port adapter sends the accounting statistics to the RP. When using NHRP in distributed CEF switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Defaults

load-interval: 30 seconds

update-rate: 10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The thresholds in the **ip nhrp trigger-svc** command must be exceeded during a certain time interval, which is 30 seconds by default. To change that interval, use the **load-interval** *seconds* argument of the **ip cef traffic-statistics** command.

When NHRP is configured on a CEF switching node with a VIP2 adapter, you must make sure the **update-rate** is set to 5 seconds.

Other features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

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 Cisco IOS software 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.

ip classless

no ip classless

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The default behavior changed from disabled to enabled.

Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When the ip classless feature is disabled, the software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, if there is no such subnet number in the routing table and there is no network default route.



Note

If the supernet, or default route, is learned via IS-IS or OSPF, the **no ip classless** configuration command is ignored.

Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip default-gateway

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 default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the router.
---------------------------	-------------------	---------------------------

Defaults	Disabled
-----------------	----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an ICMP Redirect message back. The ICMP Redirect message indicates which local router the Cisco IOS software should use.
-------------------------	--

Examples	The following example defines the router on IP address 192.31.7.18 as the default router:
-----------------	---

```
ip default-gateway 192.31.7.18
```

Related Commands	Command	Description
	ip redirects	Enables the sending of ICMP Redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
	show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP Redirect message has been received.

ip directed-broadcast

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.

ip directed-broadcast [*access-list-number*] | [*extended access-list-number*]

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

Syntax Description		
<i>access-list-number</i>	(Optional) Standard access list number in the range from 1 to 199.	If specified, a broadcast must pass the access list to be forwarded.
<i>extended access-list-number</i>	(Optional) Extended access list number in the range from 1300 to 2699.	

Defaults Disabled; all IP directed broadcasts are dropped.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	The default behavior changed to directed broadcasts being dropped.

Usage Guidelines An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is “exploded” as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** interface command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

**Note**

Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

Examples

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ip directed-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip domain-list

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.

ip domain-list *name*

no ip domain-list *name*

Syntax Description

<i>name</i>	Domain name. Do not include the initial period that separates an unqualified name from the domain name.
-------------	---

Defaults

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If there is no domain list, the domain name that you specified with the **ip domain-name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain-list** command is similar to the **ip domain-name** command, except that with **ip domain-list** you can define a list of domains, each to be tried in turn.

Examples

The following example adds several domain names to a list:

```
ip domain-list martinez.com
ip domain-list stanford.edu
```

The following example adds a name to and then deletes a name from the list:

```
ip domain-list sunya.edu
no ip domain-list stanford.edu
```

Related Commands

Command	Description
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).

ip domain-lookup

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

ip domain-lookup

no ip domain-lookup

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example enables the IP Domain Naming System-based host name-to-address translation:

```
ip domain-lookup
```

Related Commands	Command	Description
	ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
	ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain-name

To define a default domain name that the Cisco IOS software 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 DNS, use the **no** form of this command.

ip domain-name *name*

no ip domain-name

Syntax Description	<i>name</i>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.
---------------------------	-------------	---

Defaults	Enabled
-----------------	---------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Any IP host name that does not contain a domain name (that is, any name without a dot), will have the dot and cisco.com appended to it before being added to the host table.
-------------------------	--

Examples	The following example defines cisco.com as the default domain name: <pre>ip domain-name cisco.com</pre>
-----------------	--

Related Commands	Command	Description
	ip domain-list	Defines a list of default domain names to complete unqualified host names.
	ip domain-lookup	Enables the IP DNS-based host name-to-address translation.
	ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip forward-protocol

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.

```
ip forward-protocol { udp [port] | nd | sdns }
```

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

Syntax Description

udp	Forward User Datagram Protocol (UDP) datagrams. See the “Default” section below for a list of port numbers forwarded by default.
<i>port</i>	(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.

Defaults

If an IP helper address is defined, UDP forwarding is enabled on default ports. If UDP flooding is configured, UDP flooding is enabled on the default ports.

If a helper address is specified and UDP forwarding is enabled, broadcast packets destined to the following port numbers are forwarded by default:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)
- TACACS service (port 49)
- IEN-116 Name Service (port 42)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

ip forward-protocol spanning-tree [**any-local-broadcast**]

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

Syntax Description	any-local-broadcast (Optional) Accept any local broadcast when flooding.				
Defaults	Disabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.
Release	Modification				
10.0	This command was introduced.				

Usage Guidelines

A packet must meet the following criteria to be considered for flooding:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; major-net broadcast for the receiving interface if the **no ip classless** command is also configured; or any local IP broadcast address if the **ip forward-protocol spanning-tree any-local-broadcast** command is configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, or BOOTP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any desired address. Thus, the destination address may change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

After a decision has been made to send the datagram out on an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is therefore subject to access lists, if they are present on the output interface.

The **ip forward-protocol spanning-tree** command uses the database created by the bridging spanning-tree protocol. Therefore, the transparent bridging option must be in the routing software, and bridging must be configured on each interface that is to participate in the flooding in order to support this capability.

If an interface does not have bridging configured, it still will be able to receive broadcasts, but it will never forward broadcasts received on that interface. Also, it will never use that interface to send broadcasts received on a different interface.

If no actual bridging is desired, you can configure a type-code bridging filter that will deny all packet types from being bridged. Refer to the “Configuring Transparent Bridging” chapter in the *Bridging and IBM Networking Configuration Guide* for more information about using access lists to filter bridged traffic. The spanning-tree database is still available to the IP forwarding code to use for the flooding.

The spanning-tree-based flooding mechanism forwards packets whose contents are all ones (255.255.255.255), all zeros (0.0.0.0), and, if subnetting is enabled, all networks (131.108.255.255 as an example in the network number 131.108.0.0). This mechanism also forward packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 131.108.0.0).

This command is an extension of the **ip helper-address** interface configuration command, in that the same packets that may be subject to the helper address and forwarded to a single network can now be flooded. Only one copy of the packet will be put on each network segment.

Examples

The following example permits IP broadcasts to be flooded through the internetwork in a controlled fashion:

```
ip forward-protocol spanning-tree
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
ip forward-protocol turbo-flood	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

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.

ip forward-protocol turbo-flood

no ip forward-protocol turbo-flood

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Used in conjunction with the **ip forward-protocol spanning-tree** global configuration command, this feature is supported over Advanced Research Projects Agency (ARPA)-encapsulated Ethernets, FDDI, and HDLC-encapsulated serials, but is not supported on Token Rings. As long as the Token Rings and the non-HDLC serials are not part of the bridge group being used for UDP flooding, turbo flooding will behave normally.

Examples The following is an example of a two-port router using this feature:

```
ip forward-protocol turbo-flood
ip forward-protocol spanning-tree
!
interface ethernet 0
 ip address 128.9.1.1
 bridge-group 1
!
interface ethernet 1
 ip address 128.9.1.2
 bridge-group 1
!
bridge 1 protocol dec
```

Related Commands	Command	Description
	ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
	ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

ip helper-address

To have the Cisco IOS software 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.

ip helper-address *address*

no ip helper-address *address*

Syntax Description	<i>address</i>	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
---------------------------	----------------	---

Defaults	Disabled
-----------------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Combined with the **ip forward-protocol** global configuration command, the **ip helper-address** command allows you to control which broadcast packets and which protocols are forwarded.



Note

In order for the **ip helper-address** command to function correctly, the **ip bootp server** command must be enabled.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the router. The DHCP server now receives broadcasts from the DHCP clients.

All of the following conditions must be met in order for a UDP or IP packet to be helpered by the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.

- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

**Note**

The **ip helper-address** command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

Examples

The following example defines an address that acts as a helper address:

```
interface ethernet 1
 ip helper-address 121.24.43.2
```

Related Commands

Command	Description
ip bootp server	Enables the BOOTP service available from hosts on the network.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip host

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.

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

```
no ip host name address1
```

Syntax Description

<i>name</i>	Name of the host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
<i>tcp-port-number</i>	(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).
<i>address1</i>	Associated IP address.
<i>address2...address8</i>	(Optional) Additional associated IP address. You can bind up to eight addresses to a host name.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
ip host croff 192.31.7.18
ip host bisso-gw 10.2.0.2 192.31.7.33
```

ip host-routing

To configure your communication server to act as a terminal server, use the **ip host-routing** global configuration command. To disable host-based routing, use the **no** form of this command.

ip host-routing

no ip host-routing

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The functionality of this command compares to the functionality of the **ip routing** command as follows:

ip routing—Run the configured routing protocols. If communication servers are not configured do not send packets.

no ip routing—Do not run routing protocols. If the destination is not on the same subnet, use ARP and depend on proxies.

ip host-routing—Do not run routing protocols. If you are not on the same subnet, use ARP and depend on proxies. This command allows IP routing between the SLIP and PPP hosts attached to the communication server but uses host routing methods to send packets to devices and networks that are not directly attached.

Examples

The following example uses the **ip host-routing** command to configure the communication server to act as a terminal server:

```
ip host-routing
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
ip routing	Enables IP routing.

ip hp-host

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.

ip hp-host *hostname ip-address*

no ip hp-host *hostname ip-address*

Syntax Description

<i>hostname</i>	Name of the host.
<i>ip-address</i>	IP address of the host.

Defaults

No host names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To use the HP Proxy service, you must first enter the host name of the HP host into the host table using this command.

Examples

The following example specifies an HP host's name and address, and then enables Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface ethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip probe proxy	Enables the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy Name requests.

ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** interface configuration command. To disable IRDP routing, use the **no** form of this command.

ip irdp [**multicast** | **holdtime** *seconds* | **maxadvertinterval** *seconds* | **minadvertinterval** *seconds* | **preference** *number* | **address** *address* [*number*]]

no ip irdp

Syntax Description	
multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
holdtime <i>seconds</i>	(Optional) Length of time in seconds advertisements are held valid. Default is three times the maxadvertinterval value. Must be greater than maxadvertinterval and cannot be greater than 9000 seconds.
maxadvertinterval <i>seconds</i>	(Optional) Maximum interval in seconds between advertisements. The default is 600 seconds.
minadvertinterval <i>seconds</i>	(Optional) Minimum interval in seconds between advertisements. The default is 0.75 times the maxadvertinterval . If you change the maxadvertinterval value, this value defaults to three-quarters of the new value.
preference <i>number</i>	(Optional) Preference value. The allowed range is -2^{31} to 2^{31} . The default is 0. A higher value increases the router's preference level. You can modify a particular router so that it will be the preferred router to which others home.
address <i>address</i> [<i>number</i>]	(Optional) IP address (<i>address</i>) to proxy-advertise, and optionally, its preference value (<i>number</i>).

Defaults

Disabled

When enabled, IRDP uses these defaults:

- Broadcast IRDP advertisements
- Maximum interval between advertisements: 600 seconds
- Minimum interval between advertisements: 0.75 times **maxadvertinterval**
- Preference: 0

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If you change **maxadvertinterval**, the other two values also change, so it is important to change **maxadvertinterval** first before changing either **holdtime** or **minadvertinterval**.

The **ip irdp multicast** command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.

Examples

The following example sets the various IRDP processes:

```
! enable irdp on interface Ethernet 0
interface ethernet 0
 ip irdp
! send IRDP advertisements to the multicast address
 ip irdp multicast
! increase router preference from 100 to 50
 ip irdp preference 50
! set maximum time between advertisements to 400 secs
 ip irdp maxadvertinterval 400
! set minimum time between advertisements to 100 secs
 ip irdp minadvertinterval 100
! advertisements are good for 6000 seconds
 ip irdp holdtime 6000
! proxy-advertise 131.108.14.5 with default router preference
 ip irdp address 131.108.14.5
! proxy-advertise 131.108.14.6 with preference of 50
 ip irdp address 131.108.14.6 50
```

Related Commands

Command	Description
show ip irdp	Displays IRDP values.

ip mobile arp

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.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

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

Syntax Description		
timers	(Optional)	Indicates that you are setting local-area mobility timers.
<i>keepalive</i>	(Optional)	Frequency, in minutes, at which the Cisco IOS software sends unicast ARP messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 5 minutes (300 seconds).
<i>hold-time</i>	(Optional)	Hold time, in minutes. This is the length of time the software 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 15 minutes (300 seconds).
access-group	(Optional)	Indicates that you are applying an access list. This access list applies only to local-area mobility.
<i>access-list-number</i>	(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.
<i>name</i>	(Optional)	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Defaults

Local-area mobility is disabled.

If you enable local-area mobility:

keepalive: 5 minutes (300 seconds)

hold-time: 15 minutes (900 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, OSPF, or Intermediate System-to-Intermediate System (IS-IS); you can also use RIP, but this is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be taken for mobile nodes and disrupt normal operations.

Examples

The following example configures local-area mobility on Ethernet interface 0:

```
access-list 10 permit 198.92.37.114
interface ethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip name-server

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.

```
ip name-server server-address1 [server-address2...server-address6]
```

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

Syntax Description

<i>server-address1</i>	IP addresses of name server.
<i>server-address2...server-address6</i>	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Defaults

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example specifies host 131.108.1.111 as the primary name server and host 131.108.1.2 as the secondary server:

```
ip name-server 131.108.1.111 131.108.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 131.108.1.111
ip name-server 131.108.1.2
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).

ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), use the **ip nat** interface configuration command. To prevent the interface from being able to translate, use the **no** form of this command.

```
ip nat {inside | outside} | log {translations syslog}
```

```
no ip nat {inside | outside} | log {translations syslog}
```

Syntax Description

inside	Indicates the interface is connected to the inside network (the network subject to NAT translation).
outside	Indicates the interface is connected to the outside network.
log	Enables NAT logging.
translations	Enables NAT logging translations.
syslog	Enables syslog for NAT logging translations.

Defaults

Traffic leaving or arriving at this interface is not subject to network address translation.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Only packets moving between “inside” and “outside” interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

NAT translations logging can be enabled or disabled with the **ip nat log translations syslog** command.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 networks to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands	Command	Description
	clear ip nat translation	Clears dynamic NAT translations from the translation table.
	ip nat inside destination	Enables NAT of the inside destination address.
	ip nat inside source	Enables NAT of the inside source address.
	ip nat outside source	Enables NAT of the outside source address.
	ip nat pool	Defines a pool of IP addresses for NAT.
	ip nat service	Enables a port other than the default port.
	ip nat translation	Changes the amount of time after which NAT translations time out.
	show ip nat statistics	Displays NAT statistics.
	show ip nat translations	Displays active NAT translations.

ip nat inside destination

To enable Network Address Translation (NAT) of the inside destination address, use the **ip nat inside destination** global configuration command. To remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside destination list {*access-list-number* | *name*} **pool** *name*

no ip nat inside destination list {*access-list-number* | *name*}

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
list <i>name</i>	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated during dynamic translation.

Defaults

No inside destination addresses are translated.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Examples

The following example translates between inside hosts addressed to either the 192.168.1.0 or 192.168.2.0 networks to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside destination list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

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

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** global configuration command. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

```
ip nat inside source {list {access-list-number | name} pool name [overload] | static local-ip global-ip}
```

```
no ip nat inside source {list {access-list-number | name} pool name [overload] | static local-ip global-ip}
```

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list <i>name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, each inside host's TCP or UDP port number distinguishes between the multiple conversations using the same local IP address.
static <i>local-ip</i>	Sets up a single static translation; this argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>global-ip</i>	Sets up a single static translation; this argument establishes the globally unique IP address of an inside host as it appears to the outside world.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 networks to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

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

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** global configuration command. To remove the static entry or the dynamic association, use the **no** form of this command.

ip nat outside source {**list** {*access-list-number* | *name*} **pool** *name* | **static** *global-ip local-ip*}

no ip nat outside source {**list** {*access-list-number* | *name*} **pool** *name* | **static** *global-ip local-ip*}

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list <i>name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated.
static <i>global-ip</i>	Sets up a single static translation. This argument establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
<i>local-ip</i>	Sets up a single static translation. This argument establishes the local IP address of an outside host as it appears to the inside world. The address was allocated from address space routable on the inside (RFC 1918, perhaps).

Defaults

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this feature if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Examples

The following example translates between inside hosts addressed from the 9.114.11.0 network to the globally unique 171.69.233.208/28 network. Further packets from outside hosts addressed from the 9.114.11.0 network (the true 9.114.11.0 network) are translated to appear to be from the network 10.0.1.0/24.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool** global configuration command. To remove one or more addresses from the pool, use the **no** form of this command.

```
ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary]
```

```
no ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary]
```

Syntax Description

<i>name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
netmask <i>netmask</i>	Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
prefix-length <i>prefix-length</i>	Number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
type rotary	(Optional) Indicates that the range of address in the address pool identify real, inside hosts among which TCP load distribution will occur.

Defaults

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define either an inside global pool, an outside local pool, or a rotary pool.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 networks to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.
ip nat translation	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service

To specify a port other than the default port, use the **ip nat service** global configuration command. To disable the port, use the **no** form of this command.

```
ip nat service {list {access-list-number | access-list-name} ftp tcp port port-number}
```

```
no ip nat service {list {access-list-number | access-list-name} ftp tcp port port-number}
```

list access-list number	Standard access list number in the range from 1 to 199.
access-list-name	Name of a standard IP access list.
ftp	FTP protocol.
tcp	TCP protocol.
port port-number	Port other than the default port in the range from 1 to 65533.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

Examples

The following example configures the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.

Command	Description
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat translation

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** global configuration command. To disable the timeout, use the **no** form of this command.

```
ip nat translation [max-entries number] {timeout | udp-timeout | dns-timeout | tcp-timeout |
finrst-timeout | icmp-timeout | pptp-timeout | syn-timeout | port-timeout}
seconds | never
```

```
no ip nat translation [max-entries number] {timeout | udp-timeout | dns-timeout | tcp-timeout
| finrst-timeout | icmp-timeout | pptp-timeout | syn-timeout | port-timeout}
```

Syntax Description	
max-entries <i>number</i>	(Optional) Specifies the maximum number (1-2147483647) of NAT entries. Default is unlimited.
timeout	Specifies that the timeout value applies to dynamic translations except for overload translations. Default is 86400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the UDP port. Default is 300 seconds (5 minutes).
dns-timeout	Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86400 seconds (24 hours).
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
pptp-timeout	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. Default is 86400 seconds (24 hours).
syn-timeout	Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
<i>seconds</i>	Number of seconds after which the specified port translation times out. Default values are listed in the Default section.
<i>never</i>	Specifies no port translation time out.

Defaults

timeout is 86400 seconds (24 hours)
udp-timeout is 300 seconds (5 minutes)
dns-timeout is 60 seconds (1 minute)
tcp-timeout is 86400 seconds (24 hours)
finrst-timeout is 60 seconds (1 minute)
icmp-timeout is 60 seconds (1 minute)

pptp-timeout is 86400 seconds (24 hours)

syn-timeout is 60 seconds (1 minute)

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When port translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it. Non-Domain Naming System UDP translations time out after 5 minutes, while DNS times out in 1 minute. TCP translations timeout in 24 hours, unless a RST or FIN is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example causes UDP port translation entries to timeout after 10 minutes:

```
ip nat translation udp-timeout 600
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip netmask-format

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.

```
ip netmask-format {bit-count | decimal | hexadecimal}
```

```
no ip netmask-format [bit-count | decimal | hexadecimal]
```

Syntax Description

bit-count	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).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0FFFFFFF00).

Defaults

Netmasks are displayed in bitcount format.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.0 0FFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.0/24.

Examples

The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

ip nhrp authentication

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.

ip nhrp authentication *string*

no ip nhrp authentication [*string*]

Syntax Description

<i>string</i>	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.
---------------	---

Defaults

No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

All routers configured with NHRP within one logical NBMA network must share the same authentication string.

Examples

In the following example, the authentication string named *specialxx* must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication specialxx
```

ip nhrp holdtime

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.

ip nhrp holdtime *seconds*

no ip nhrp holdtime [*seconds*]

Syntax Description	<i>seconds</i>	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses.
---------------------------	----------------	---

Defaults	7200 seconds (2 hours)
-----------------	------------------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines The **ip nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

Examples In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for one hour:

```
ip nhrp holdtime 3600
```

ip nhrp interest

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.

ip nhrp interest *access-list-number*

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

Syntax Description

<i>access-list-number</i>	Standard or extended IP access list number in the range 1 to 199.
---------------------------	---

Defaults

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command with the **access-list** command to control which IP packets trigger NHRP Requests. The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, any TCP traffic can cause NHRP Requests to be sent, but no other IP packets will cause NHRP Requests:

```
ip nhrp interest 101
access-list 101 permit tcp any any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp map

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 nhrp map *ip-address nbma-address*

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

Syntax Description

<i>ip-address</i>	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
<i>nbma-address</i>	NBMA address that 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.

Defaults

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You will probably have to configure at least one static mapping in order to reach the Next Hop Server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two Next Hop Servers 100.0.0.1 and 100.0.1.3. The NBMA address for 100.0.0.1 is statically configured to be 11.0.0.1 and the NBMA address for 100.0.1.3 is 12.2.7.8.

```
interface tunnel 0
 ip nhrp nhs 100.0.0.1
 ip nhrp nhs 100.0.1.3
 ip nhrp map 100.0.0.1 11.0.0.1
 ip nhrp map 100.0.1.3 12.2.7.8
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.

ip nhrp map multicast

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.

ip nhrp map multicast *nbma-address*

no ip nhrp map multicast *nbma-address*

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

Defaults	No NBMA addresses are configured as destinations for broadcast or multicast packets.
-----------------	--

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	<p>This command applies only to tunnel interfaces.</p> <p>The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the tunnel destination command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.</p> <p>When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.</p>
-------------------------	---

Examples	<p>In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 11.0.0.1 and 11.0.0.2. Addresses 11.0.0.1 and 11.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.</p>
-----------------	--

```
interface tunnel 0
ip address 10.0.0.3 255.0.0.0
ip nhrp map multicast 11.0.0.1
ip nhrp map multicast 11.0.0.2
```

ip nhrp max-send

To change the maximum frequency at which NHRP packets can be sent, use the **ip nhrp max-send** interface configuration command. To restore this frequency to the default value, use the **no** form of this command.

ip nhrp max-send *pkt-count* **every** *interval*

no ip nhrp max-send

Syntax Description		
	<i>pkt-count</i>	Number of packets which can be transmitted in the range from 1 to 65535. Default is 5 packets.
	every <i>interval</i>	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults	
	<i>pkt-count</i> = 5 packets
	<i>interval</i> = 10 seconds

Command Modes	
	Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	
	The software maintains a per-interface quota of NHRP packets that can be transmitted. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by <i>interval</i> .

Examples	
	In the following example, only 1 NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ip nhrp max-send 1 every 60
```

Related Commands	Command	Description
	ip nhrp interest	Controls which IP packets can trigger sending a NHRP request.
	ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp network-id

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.

ip nhrp network-id *number*

no ip nhrp network-id [*number*]

Syntax Description	<i>number</i>	Globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295.
---------------------------	---------------	--

Defaults	NHRP is disabled on the interface.
-----------------	------------------------------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.
-------------------------	--

Examples	The following example enables NHRP on the interface:
-----------------	--

```
ip nhrp network-id 1
```

ip nhrp nhs

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.

```
ip nhrp nhs nhs-address [net-address [netmask]]
```

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

Syntax Description

<i>nhs-address</i>	Address of the Next Hop Server being specified.
<i>net-address</i>	(Optional) IP address of a network served by the Next Hop Server.
<i>netmask</i>	(Optional) IP network mask to be associated with the <i>net</i> IP address. The <i>net</i> IP address is logically ANDed with the mask.

Defaults

No Next Hop Servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to specify the address of a Next Hop Server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When Next Hop Servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any Next Hop Server that is configured, you can specify multiple networks that it serves by repeating this command with the same *nhs-address*, but with different *net-address* IP network addresses.

Examples

In the following example, the Next Hop Server with address 131.108.10.11 serves IP network 10.0.0.0. The mask is 255.0.0.0.

```
ip nhrp nhs 131.108.10.11 10.0.0.0 255.0.0.0
```

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 record

no ip nhrp record

Syntax Description

This command has no arguments or keywords.

Defaults

Forward record and reverse record options are used in NHRP Request and Reply packets.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ip nhrp responder** command.

Examples

The following example suppresses forward record and reverse record options:

```
no ip nhrp record
```

Related Commands

Command	Description
ip nhrp responder	Designates the primary IP address of which interface the Next Hop Server will use in NHRP Reply packets when the NHRP requester uses the Responder Address option.

ip nhrp responder

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.

ip nhrp responder *type number*

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

Syntax Description

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

Defaults

The Next Hop Server uses the IP address of the interface where the NHRP Request was received.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If an NHRP requestor wants to know which Next Hop Server generates an NHRP Reply packet, it can request that information through the Responder Address option. The Next Hop Server that generates the NHRP Reply packet then complies by inserting its own IP address in the Responder Address option of the NHRP Reply. The Next Hop Server uses the primary IP address of the specified interface.

If an NHRP Reply packet being forwarded by a Next Hop Server contains that Next Hop Server's own IP address, the Next Hop Server generates an Error Indication of type "NHRP Loop Detected" and discards the Reply.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a Next Hop Server to supply the primary IP address of serial interface 0 in the NHRP Reply packet:

```
ip nhrp responder serial 0
```

ip nhrp server-only

To configure the interface to operate in NHRP server-only mode, use the **ip nhrp server-only** interface configuration command. To disable this feature, use the **no** form of this command.

ip nhrp server-only [non-caching]

no ip nhrp server-only

Syntax Description	non-caching (Optional) The router will not cache NHRP information received on this interface.
---------------------------	--

Defaults	Disabled
-----------------	----------

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

Command History	Release	Modification
	11.2	This command was introduced.
	12.0	The non-caching keyword was added.

Usage Guidelines	When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut SVC.
-------------------------	--

Examples	The following example configures the interface to operate in server-only mode: <pre>ip nhrp server-only</pre>
-----------------	--

ip nhrp trigger-svc

To configure when Next Hop Resolution Protocol (NHRP) will set up and tear down an SVC based on aggregate traffic rates, use the **ip nhrp trigger-svc** interface configuration command. To restore the default thresholds, use the **no** form of this command.

```
ip nhrp trigger-svc trigger-threshold teardown-threshold
```

```
no ip nhrp trigger-svc
```

Syntax Description

<i>trigger-threshold</i>	Average traffic rate calculated during the load-interval , at or above which NHRP will set up an SVC for a destination. The default value is 1 kbps.
<i>teardown-threshold</i>	Average traffic rate calculated during the load-interval , at or below which NHRP will tear down the SVC to the destination. The default value is 0 kbps.

Defaults

trigger-threshold: 1 kbps

teardown-threshold: 0 kbps

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default. To change that interval, use the **load-interval seconds** argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kbps and 5 kbps, respectively:

```
ip nhrp trigger-svc 100 5
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.
ip cef accounting	Enables network accounting of CEF information.
ip cef traffic-statistics	Changes the time interval that controls when NHRP will set up or tear down an SVC.
ip nhrp interest	Controls which IP packets can trigger sending a NHRP request.

ip nhrp use

To configure the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ip nhrp use** interface configuration command. To restore the default value, use the **no** form of this command.

ip nhrp use *usage-count*

no ip nhrp use *usage-count*

Syntax Description

<i>usage-count</i>	Packet count in the range from 1 to 65535. Default is 1.
--------------------	--

Defaults

usage-count = 1. The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

When the software attempts to transmit a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally transmitted right away. Configuring the *usage-count* causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The *usage-count* applies *per destination*. So if *usage-count* is configured to be 3, and 4 data packets are sent toward 10.0.0.1 and 1 packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests are performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute 4 packets are sent to one destination and 5 packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system retransmits its request for the second destination.

```
ip nhrp use 5
```

Related Commands	Command	Description
	ip nhrp interest	Controls which IP packets can trigger sending a NHRP request.
	ip nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ip probe proxy

To enable the HP Probe Proxy support, which allows the Cisco IOS software 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.

ip probe proxy

no ip probe proxy

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines HP Probe Proxy Name requests are typically used at sites that have HP equipment and are already using HP Probe.

To use the HP Proxy service, you must first enter the host name of the HP host into the host table using the **ip hp-host** global configuration command.

Examples The following example specifies an HP host's name and address, and then enables Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface ethernet 0
ip probe proxy
```

Related Commands	Command	Description
	ip hp-host	Enters into the host table the host name of an HP host to be used for HP Probe Proxy service.

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.

ip proxy-arp

no ip proxy-arp

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
 ip proxy-arp
```

ip routing

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

ip routing

no ip routing

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines If Concurrent Routing and Bridging (CRB) is configured, this command is unnecessary because all protocols are bridged by default. If CRB is not configured, configure the **no ip routing** command to bridge IP.

The **ip routing** command is disabled on the Cisco VG200 voice over IP gateway.

Examples The following example enables IP routing:

```
ip routing
```

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.

ip subnet-zero

no ip subnet-zero

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **ip subnet-zero** command provides the ability to configure and route to subnet-zero subnets. Subnetting with a subnet address of zero is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

Examples The following example enables subnet-zero:

```
ip subnet-zero
```

ip unnumbered

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.

ip unnumbered *type number*

no ip unnumbered *type number*

Syntax Description	<i>type number</i>	Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.
---------------------------	--------------------	---

Defaults	Disabled
-----------------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- Serial interfaces using HDLC, PPP, Link Access Procedure, Balanced (LAPB), and Frame Relay encapsulations, as well as Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping EXEC** command to determine whether the interface is up, because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- You cannot netboot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and *number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

If you are configuring IS-IS across a serial line, you should configure the serial interfaces as unnumbered. This allows you to conform with RFC 1195, which states that IP addresses are not required on each interface.

**Note**

Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, then any routing protocol running across the serial line must not advertise subnet information.

Examples

In the following example, the first serial interface is given Ethernet 0's address:

```
interface ethernet 0
 ip address 131.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered ethernet 0
```

no ip gratuitous-arps

To disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool, use the **no ip gratuitous-arps** global configuration command.

no ip gratuitous-arps

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines A Cisco router will send out a gratuitous ARP message when a client connects and negotiates an address over a PPP connection. This transmission occurs even when the client receives the address from a local address pool.

Examples The following example disables gratuitous arp messages from being sent:

```
no ip gratuitous-arps
```

show arp

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

show arp

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Release	Modification
10.0	This command was introduced.

Examples The following is sample output from the **show arp** command:

```
Router# show arp

Protocol  Address          Age (min)  Hardware Addr  Type   Interface
-----
Internet  131.108.42.112  120       0000.a710.4baf ARPA   Ethernet3
AppleTalk 4028.5           29        0000.0c01.0e56 SNAP   Ethernet2
Internet  131.108.42.114  105       0000.a710.859b ARPA   Ethernet3
AppleTalk 4028.9           -         0000.0c02.a03c SNAP   Ethernet2
Internet  131.108.42.121  42        0000.a710.68cd ARPA   Ethernet3
Internet  131.108.36.9    -         0000.3080.6fd4 SNAP   TokenRing0
AppleTalk 4036.9           -         0000.3080.6fd4 SNAP   TokenRing0
Internet  131.108.33.9    -         0000.0c01.7bbd SNAP   Fddi0
```

Table 3 describes significant fields shown in the first line of output in the display.

Table 3 *show arp Field Descriptions*

Field	Description
Protocol	Indicates the type of network address this entry includes.
Address	Network address that is mapped to the MAC address in this entry.
Age (min)	Indicates the interval (in minutes) since this entry was entered in the table, rather than the interval since the entry was last used. (The timeout value is 4 hours.)
Hardware Addr	MAC address mapped to the network address in this entry.

Table 3 *show arp Field Descriptions (continued)*

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: <ul style="list-style-type: none">• ARPA• SNAP• ETLK (EtherTalk)• SMDS
Interface	Indicates the interface associated with this network address.

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 hosts

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following is sample output from the **show hosts** command:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host          Flag      Age   Type      Address(es)
SLAG.CISCO.COM (temp, OK) 1     IP        131.108.4.10
CHAR.CISCO.COM (temp, OK) 8     IP        192.31.7.50
CHAOS.CISCO.COM (temp, OK) 8     IP        131.108.1.115
DIRT.CISCO.COM (temp, EX) 8     IP        131.108.1.111
DUSTBIN.CISCO.COM (temp, EX) 0     IP        131.108.1.27
DREGS.CISCO.COM (temp, EX) 24    IP        131.108.1.30
```

Table 4 describes significant fields shown in the display.

Table 4 *show hosts Field Descriptions*

Field	Description
Flag	A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. A permanent entry is entered by a configuration command and is not timed out. Entries marked OK are believed to be valid. Entries marked ?? are considered suspect and subject to revalidation. Entries marked EX are expired.
Age	Indicates the number of hours since the software last referred to the cache entry.
Type	Identifies the type of address, for example, IP, CLNS, or X.121. If you have used the ip hp-host global configuration command, the show hosts command will display these host names as type HP-IP.
Address(es)	Shows the address of the host. One host may have up to eight addresses.

■ show hosts**Related Commands**

Command	Description
clear host	Deletes entries from the host-name-and-address cache.

show ip aliases

To display the 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 aliases

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Release	Modification
10.0	This command was introduced.

Usage Guidelines To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the “port” number, where 1 is the auxiliary port.

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

```
Router# show ip aliases

  IP Address      Port
131.108.29.245  SLIP TTY1
```

The display lists the IP address and corresponding port number.

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

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 arp [ip-address] [hostname] [mac-address] [type number]
```

Syntax Description		
<i>ip-address</i>	(Optional) ARP entries matching this IP address are displayed.	
<i>hostname</i>	(Optional) Host name.	
<i>mac-address</i>	(Optional) 48-bit MAC address.	
<i>type number</i>	(Optional) ARP entries learned via this interface type and number are displayed.	

Command Modes EXEC

Usage Guidelines ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

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

```
Router# show ip arp

Protocol  Address           Age (min)  Hardware Addr  Type   Interface
-----
Internet  171.69.233.22    9          0000.0c59.f892 ARPA   Ethernet0/0
Internet  171.69.233.21    8          0000.0c07.ac00 ARPA   Ethernet0/0
Internet  171.69.233.19    -          0000.0c63.1300 ARPA   Ethernet0/0
Internet  171.69.233.30    9          0000.0c36.6965 ARPA   Ethernet0/0
Internet  172.19.168.11    -          0000.0c63.1300 ARPA   Ethernet0/0
Internet  172.19.168.254  9          0000.0c36.6965 ARPA   Ethernet0/0
```

Table 5 describes significant fields shown in the display.

Table 5 *show ip arp* Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to Hardware Address.
Age (min)	Age, in minutes, of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address a MAC address that corresponds to network address.

Table 5 *show ip arp Field Descriptions (continued)*

Field	Description
Type	Type of encapsulation: <ul style="list-style-type: none">• ARPA—Ethernet• SNAP—RFC 1042• SAP—IEEE 802.3
Interface	Interface to which this address mapping has been assigned.

show ip interface

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

show ip interface [*type number*] [**brief**]

Syntax Description		
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes	
	EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network (if any).

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you will see only information on that specific interface.

If you specify no optional arguments, you will see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or SLIP, IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

Examples

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

```
Router# show ip interface

Ethernet0 is up, line protocol is up
  Internet address is 192.195.78.24, subnet mask is 255.255.255.240
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Secondary address 131.192.115.2, subnet mask 255.255.255.0
  Directed broadcast forwarding is enabled
  Multicast groups joined: 224.0.0.1 224.0.0.2
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP SSE switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
```

Table 6 describes the fields shown in the display.

Table 6 *show ip interface Field Descriptions*

Field	Description
Ethernet0 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address and subnet mask	IP Internet address and subnet mask of the interface.
Broadcast address	Shows the broadcast address.
Address determined by ...	Indicates how the IP address of the interface was determined.
MTU	Shows the MTU value set on the interface.
Helper address	Shows a helper address, if one has been set.
Secondary address	Shows a secondary address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Multicast groups joined	Indicates the multicast groups this interface is a member of.
Outgoing access list	Indicates whether the interface has an outgoing access list set.

Table 6 *show ip interface Field Descriptions (continued)*

Field	Description
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy ARP is enabled for the interface.
Security level	Specifies the IPSO security level set for this interface.
Split horizon	Indicates split horizon is enabled.
ICMP redirects	Specifies whether redirects will be sent on this interface.
ICMP unreachable	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP SSE switching	Specifies whether IP SSE switching is enabled.
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
Probe proxy name	Indicates whether HP Probe proxy name replies are generated.

show ip irdp

To display IRDP values, use the **show ip irdp** EXEC command.

show ip irdp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

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

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
--More--
Serial 0 has router discovery disabled
--More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less self-evident lines of output in the display are as follows:

Advertisements will occur between every 450 and 600 seconds.

This indicates the configured minimum and maximum advertising interval for the interface.

Advertisements are valid for 1800 seconds.

This indicates the configured holdtime values for the interface.

Default preference will be 100.

This indicates the configured (or in this case default) preference value for the interface.

Related Commands	Command	Description
	ip irdp	Enables IRDP processing on an interface.

show ip masks

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

show ip masks *address*

Syntax Description	<i>address</i>	Network address for which a mask is required.
--------------------	----------------	---

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

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

```
Router# show ip masks 131.108.0.0

Mask           Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics EXEC** command.

show ip nat statistics

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Examples The following is sample output from the **show ip nat statistics** command:

```
Router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
   start 171.69.233.208 end 171.69.233.221
   type generic, total addresses 14, allocated 2 (14%), misses 0
```

Table 7 describes the significant fields in the display.

Table 7 *show ip nat statistics Field Descriptions*

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the ip nat outside command.
Inside interfaces	List of interfaces marked as inside with the ip nat inside command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

Table 7 *show ip nat statistics Field Descriptions (continued)*

Field	Description
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations that are using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool that are available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

Related Commands

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

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations EXEC** command.

show ip nat translations [verbose]

Syntax Description	verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
--------------------	---------	---

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

Command History	Release	Modification
	11.2	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 171.69.233.209     192.168.1.95     ---               ---
--- 171.69.233.210     192.168.1.89     ---               --
```

With overloading, a translation for a DNS transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

The following is sample output that includes the **verbose** keyword.

```
Router# show ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
      create 00:00:02, use 00:00:00, flags: extended
```

Table 8 describes the significant fields in the display.

Table 8 *show ip nat translations Field Descriptions*

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are <ul style="list-style-type: none"> • extended—Extended translation • static—Static translation • destination—Rotary translation • outside—Outside translation • timing out—Translation will no longer be used, due to a TCP FIN or RST.

Related Commands

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

show ip nhrp

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

```
show ip nhrp [dynamic | static] [type number]
```

Syntax Description	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.

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Examples

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

```
Router# show ip nhrp

10.0.0.2 255.255.255.255, ATM0/0 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: 11.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: 11.1.1.2
```

Table 9 describes the fields in the display.

Table 9 show ip nhrp Field Descriptions

Field	Description
100.0.0.2 255.255.255.255	IP address and its network mask in the IP-to-NBMA address cache. The mask is currently always 255.255.255.255 because we do not support aggregation of NBMA information through NHRP.
ATM0/0 created 0:00:43	Interface type and number (in this case, ATM slot and port numbers) and how long ago it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the ip nhrp holdtime command.

Table 9 *show ip nhrp Field Descriptions (continued)*

Field	Description
Type	Value can be one of the following: <ul style="list-style-type: none"> • dynamic—NBMA address was obtained from NHRP Request packet. • static—NBMA address was statically configured.
Flags	Value can be one of the following: <ul style="list-style-type: none"> • authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination. • implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router. • negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.
NBMA address	Nonbroadcast, multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, SMDS, multipoint tunnel).

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ip nhrp traffic

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

show ip nhrp traffic

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Examples The following is sample output from the **show ip nhrp traffic** command:

```
Router# show ip nhrp traffic
Tunnel0
  request packets sent: 2
  request packets received: 4
  reply packets sent: 4
  reply packets received: 2
  register packets sent: 0
  register packets received: 0
  error packets sent: 0
  error packets received: 0
Router#
```

Table 10 describes the fields in the display.

Table 10 show ip nhrp traffic Field Descriptions

Field	Description
Tunnel 0	Interface type and number.
request packets sent	Number of NHRP Request packets originated from this station.
request packets received	Number of NHRP Request packets received by this station.
reply packets sent	Number of NHRP Reply packets originated from this station.
reply packets received	Number of NHRP Reply packets received by this station.
register packets sent	Number of NHRP Register packets originated from this station. Currently, our routers and access servers do not send Register packets, so this value is 0.
register packets received	Number of NHRP Register packets received by this station. Currently, our routers or access servers do not send Register packets, so this value is 0.

Table 10 *show ip nhrp traffic Field Descriptions (continued)*

Field	Description
error packets sent	Number of NHRP Error packets originated by this station.
error packets received	Number of NHRP Error packets received by this station.

term ip netmask-format

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.

```
term ip netmask-format {bitcount | decimal | hexadecimal}
```

```
term no ip netmask-format [bitcount | decimal | hexadecimal]
```

Syntax Description	bitcount	decimal	hexadecimal
	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.	Netmasks are displayed in dotted decimal notation (for example, 255.255.255.0).	Netmasks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0FFFFFFF00).

Defaults Netmasks are displayed in dotted decimal format.

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0FFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

Examples The following example specifies that network masks for the session be displayed in bitcount notation in the output of **show** commands:

```
term ip netmask-format bitcount
```

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.

tunnel mode { **aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** [**multipoint**] | **ipip** | **nos** }

no tunnel mode

Syntax Description		
aurp		AppleTalk Update-Based Routing Protocol (AURP).
cayman		Cayman TunnelTalk AppleTalk encapsulation.
dvmrp		Distance Vector Multicast Routing Protocol.
eon		EON compatible CLNS tunnel.
gre ip		Generic routing 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.
ipip		IP over IP encapsulation.
nos		KA9Q/NOS compatible IP over IP.

Defaults GRE tunneling

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The ipip keyword was introduced.

Usage Guidelines You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman tunneling implements tunneling as designed by Cayman Systems. This enables our routers and access servers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between our device and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address. This means that there is no way to ping the other end of the tunnel.

Use Distance Vector Multicast Routing Protocol (DVMRP) when a router connects to an mrouter to run DVMRP over a tunnel. It is required to configure Protocol-Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

Generic routing encapsulation (GRE) tunneling can be done between our routers and access servers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. This means that you can ping the other end of the tunnel.

Examples

For multipoint GRE tunnels, a tunnel key must be configured. Unlike other tunnels, the tunnel destination is optional. However, if the tunnel destination is supplied, it must map to an IP multicast address.

The following example enables Cayman tunneling:

```
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination 131.108.164.19
 tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel 0
 appletalk cable-range 4160-4160 4160.19
 appletalk zone Engineering
 tunnel source ethernet 0
 tunnel destination 131.108.164.19
 tunnel mode gre ip
```

