

ip mask-reply

To have the Cisco IOS software respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ip mask-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip mask-reply

no ip mask-reply

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.

Examples

The following example enables the sending of ICMP mask reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 131.108.1.0 255.255.255.0
 ip mask-reply
```

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. 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 Address Resolution Protocol (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 (900 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, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP 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 mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description

bytes MTU in bytes.

Defaults

Minimum is 128 bytes; maximum depends on the interface medium.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it. All devices on a physical medium must have the same protocol MTU in order to operate.



Note

Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

Examples

The following example sets the maximum IP packet size for the first serial interface to 300 bytes:

```
interface serial 0
 ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

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** command in 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 the hosts 131.108.1.111 and 131.108.1.2 as name servers:

```
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 create flow-entries [{inside | outside}] | log {translations syslog}
```

```
no ip nat create flow-entries {inside | outside} | log {translations syslog}
```

Syntax Description

create	Creates flow entries.
flow-entries	NAT flow-based entries.
inside	Indicates that the interface is connected to the inside network (the network subject to NAT translation).
outside	Indicates that 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 NAT.

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 network 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.
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** command in global configuration mode. 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 network 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
```

■ ip nat inside destination

```
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.
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** command in global configuration mode. 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 | access-list-name} | route-map name} {interface
type number | pool name} [mapping-id map-name | vrf name] [overload]
```

```
no ip nat inside source {list {access-list-number | access-list-name} | route-map name}
{interface type number | pool name} [mapping-id map-name | vrf name] [overload]
```

Static NAT

```
ip nat inside source {static {local-ip global-ip} [vrf name] [extendable] [no-alias] [no-payload]
[route-map] [redundancy group-name] | {esp local-ip interface type number}}
```

```
no ip nat inside source {static {local-ip global-ip} [vrf name] [extendable] [no-alias]
[no-payload] [route-map] [redundancy group-name] | {esp local-ip interface type number}}
```

Port Static NAT

```
ip nat inside source {static {tcp | udp local-ip local-port global-ip global-port} [extendable]
[no-alias] [no-payload]
```

```
no ip nat inside source {static {tcp | udp local-ip local-port global-ip global-port} [extendable]
[no-alias] [no-payload]
```

Network Static NAT

```
ip nat inside source {static {network local-network global-network mask} [extendable] [no-alias]
[no-payload]
```

```
no ip nat inside source {static {network local-network global-network mask} [extendable]
[no-alias] [no-payload]
```

Syntax Description

list <i>access-list-number</i>	Number 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.
list <i>access-list-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.
route-map <i>name</i>	Specifies the named route map.
interface <i>type</i>	Specifies the interface type for the global address.
interface <i>number</i>	Specifies the interface number for the global address.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
mapping-id <i>map-name</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
static <i>local-ip</i>	Sets up a single static translation. The <i>local-ip</i> 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.
local-port	Sets the local TCP/UDP port in a range from 1-65535.
static <i>global-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside world.
global-port	Sets the global TCP/UDP port in a range from 1-65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits an alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Establishes NAT redundancy.
esp <i>local-ip</i>	Establishes IPsec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Established the IP Network mask to be with used with subnet translations.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the route-map <i>name</i> keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the redundancy <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the no-payload keyword was added.
12.2(13)T	The interface keyword was added for static translations. The mapping-id <i>map-name</i> keyword and argument combination was added. The vrf <i>name</i> keyword and argument combination was added.

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.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

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 network 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
```

The following example translates only traffic local to the providers edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface e 0 vrf shop overload
ip nat inside source list 1 interface e 0 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf bank 0.0.0.0 0.0.0.0 192.1.1.1
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface e 1 vrf shop overload
ip nat inside source list 1 interface e 1 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 172.1.1.1 global
ip route vrf bank 0.0.0.0 0.0.0.0 172.1.1.1 global
access-list 1 permit 10.1.1.0 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.
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** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

```
ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name [mapping-id map-name | vrf name] [add-route]
```

```
no ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name [mapping-id map-name | vrf name] [add-route]
```

Static NAT

```
ip nat outside source {static global-ip local-ip} [add-route] [extendable] [no-alias]
[no-payload] [redundancy group-name]
```

```
no ip nat outside source {static global-ip local-ip} [add-route] [extendable] [no-alias]
[no-payload] [redundancy group-name]
```

Port Static NAT

```
ip nat outside source {static tcp | udp global-ip global-port local-ip local-port} [add-route]
[extendable] [no-alias] [no-payload]
```

```
no ip nat outside source {static tcp | udp global-ip global-port local-ip local-port} [add-route]
[extendable] [no-alias] [no-payload]
```

Network Static NAT

```
ip nat outside source {static network global-network local-network mask} [add-route]
[extendable] [no-alias] [no-payload]
```

```
no ip nat outside source {static network global-network local-network mask} [add-route]
[extendable] [no-alias] [no-payload]
```

Syntax Description

list <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list <i>access-list-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.
route-map <i>name</i>	Specifies a named route map.
pool <i>pool-name</i>	Name of the pool from which global IP addresses are allocated.
mapping-id <i>map-name</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN.
add-route	(Optional) Adds a static route for the outside local address.

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>	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, <i>Address Allocation for Private Internets</i>).
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the local address.
no-payload	(Optional) Prohibits the translation of embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Enables the NAT redundancy operation.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.

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.
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the redundancy <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the no-payload keyword was added.
12.2(13)T	The mapping-id <i>map-name</i> keyword and argument combination was added. The vrf <i>name</i> keyword and argument combination was added.

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 **static** keyword 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 10.0.1.0/24 network.

```
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
```

The following example shows NAT configured on the Provider Edge (PE) router with a static route to the shared service for the gold and silver Virtual Private Networks (VPNs). NAT is configured as inside source static 1- to -1 translations.

```
ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 168.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 2.2.2.1 vrf gold
ip nat inside source static 192.169.121.33 2.2.2.2 vrf silver
```

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** command in global configuration mode. 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 network 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 source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Enables NAT of the outside source address.
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 service

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

```
ip nat service { fullrange { tcp | udp } port port-number | H225 | list { access-list-number | access-list-name } { ESP spi-match | IKE preserve-port | ftp tcp port port-number } | ras | rtsp port port-number | sip { tcp | udp } port port-number | skinny tcp port port-number }
```

```
no ip nat service { H225 | list { access-list-number | access-list-name } { ESP spi-match | IKE preserve-port | ftp tcp port port-number } | ras | rtsp port port-number | sip { tcp | udp } port port-number | skinny tcp port port-number }
```

Syntax Description		
fullrange		Inside local port range from 0 to 65535.
H225		H323-H225 protocol.
list <i>access-list-number</i>		Standard access list number in the range from 1 to 199.
<i>access-list-name</i>		Name of a standard IP access list.
ESP		Security Parameter Index (SPI) matching IPSec pass-through.
spi-match		SPI matching IPSec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE		Preserve Internet Key Exchange (IKE) port, as required by some IPSec servers.
preserve-port		Preserve User Datagram Protocol (UDP) port in IKE packets.
ftp		FTP protocol.
tcp		TCP protocol.
udp		User Datagram Protocol.
port <i>port-number</i>		Port other than the default port in the range from 1 to 65533.
ras		H323-RAS protocol.
rtsp		Real Time Streaming Protocol. This protocol is enabled by default on port 554.
sip		SIP protocol.
skinny		Skinny protocol.

Defaults	
	Disabled
	RTSP is enabled

Command Modes	
	Global configuration

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	The skinny keyword was added.

Release	Modification
12.2(8)T	The sip keyword was added.
12.2(15)T	The ESP and spi-match keywords were added to enable SPI matching on outside IPsec gateways. The ike and preserve-port keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	The rtsp keyword was added.
12.3(10)	The fullrange keyword was added.

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.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

To change the default range of port groups when enabling Port Address Translation (PAT) on a router running Cisco IOS and connecting VPN clients to different VPN gateways, use the **ip nat service fullrange** 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
```

The following example configures the 20002 port of the CallManager:

```
ip nat service skinny tcp port 20002
```

The following example configures TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example configures SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

The following example configures the standard TCP source port 500 to be translated to a full range of ports:

```
ip nat service fullrange tcp port 500
```

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

ip nat stateful

To designate the members of a translation group, use the **ip nat stateful** command in global configuration mode.

```
ip nat stateful id id-number {redundancy name | {primary ip-address-primary}{backup ip-address-backup} peer ip-address-peer} mapping-id map-number}
```

```
no ip nat stateful id id-number {redundancy name | {primary ip-address-primary}{backup ip-address-backup} peer ip-address-peer} mapping-id map-number}
```

Syntax Description

id <i>id-number</i>	Establishes the members given to each router in the stateful translation group.
redundancy <i>name</i>	Establishes Hot Standby Routing Protocol (HSRP) as the method of Redundancy.
primary <i>ip-address-primary</i>	Manually establishes redundancy for the primary router.
backup <i>ip-address-backup</i>	Manually establishes redundancy for the backup router.
peer <i>ip-address-peer</i>	Specifies the ip address of the peer router in the translation group.
mapping-id <i>map-number</i>	Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

Command Modes

EXEC

Command History

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

Usage Guidelines

This command has two forms: HSRP stateful NAT translation and manual stateful NAT translation. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

Examples

The following example defines a mapping list that specifies which entries will be forwarded to peers in the group:

```
Router# ip nat stateful id 1

redundancy SNATHSRP
mapping-id 10
mapping-id 11
```

ip nat translation

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command in global configuration mode. 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 User Datagram Protocol (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 which consists of digital signals that are sent with precise clocking. 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. The default is 0.
<i>never</i>	Specifies no port translation time out.

Defaults

```
timeout: 86400 seconds (24 hours)
udp-timeout: 300 seconds (5 minutes)
dns-timeout: 60 seconds (1 minute)
tcp-timeout: 86400 seconds (24 hours)
finrst-timeout: 60 seconds (1 minute)
icmp-timeout: 60 seconds (1 minute)
pptp-timeout: 86400 seconds (24 hours)
syn-timeout: 60 seconds (1 minute)
port-timeout: 0 (never)
```

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-DNS UDP translations time out after 5 minutes, while DNS times out in 1 minute. TCP translations timeout in 24 hours, unless an 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 time out 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 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.
	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** command in line configuration mode. 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

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0FFFFFF00).

Defaults

Netmasks are displayed in dotted-decimal 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 0FFFFFF00.

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 the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** command in interface configuration mode. 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 eight 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 Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime** command in interface configuration mode. 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 1 hour:

```
ip nhrp holdtime 3600
```

ip nhrp interest

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ip nhrp interest** command in interface configuration mode. 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 from 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 multicast

To configure NonBroadcast MultiAccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** command in interface configuration mode. 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>	NBMA address that 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

This command applies only to tunnel interfaces.

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.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

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.

```
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 map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings, use the **ip nhrp map multicast dynamic** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ip nhrp map multicast dynamic

no ip nhrp map multicast dynamic

Syntax Description This command has no arguments or keywords.

Defaults This command is not enabled.

Command Modes Interface configuration

Command History

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

Usage Guidelines

Use this command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IPsec (IPSec) tunnels and register their unicast NHRP mappings. This command is needed to enable dynamic routing protocols to work over the Multipoint GRE and IPSec tunnels because IGP routing protocols use multicast packets. This command prevents the Hub router from needing a separate configuration line for a multicast mapping for each spoke router.

Examples

The following example shows how to enable the **ip nhrp map multicast dynamic** command on the hub router:

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1436
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
```

```
ip address 172.17.0.1 255.255.255.0
```

ip nhrp map

To statically configure the IP-to-NonBroadcast MultiAccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (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 a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (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 need 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 max-send

To change the maximum frequency at which Next Hop Resolution Protocol (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 that can be sent in the range from 1 to 65535. Default is 100 packets.
	every <i>interval</i>	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults	
	<i>pkt-count</i> : 100 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 sent. 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 the <i>interval value</i> .

Examples	
	In the following example, only one 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 an 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** command in interface configuration mode. 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 from a nonbroadcast multiaccess (NBMA) network. The range is from 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 Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** command in interface configuration mode. 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* argument, 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 reenable the use of forward record and reverse record options in Next Hop Resolution Protocol (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 registration no-unique

To enable the client to not set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp registration no-unique** command in interface configuration mode. To reenble this functionality, use the **no** form of this command.

ip nhrp registration no-unique

no ip nhrp registration no-unique

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

If the unique flag is set in the NHRP registration request packet, a Next Hop Server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address, for example via DHCP, and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration no-unique** command, the unique flag is not set, and the NHS can override the old registration information.

This command is useful in an environment where client IP addresses can change frequently such as a dial environment.

Examples

The following example configures the client to not set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration no-unique
```

ip nhrp responder

To designate the primary IP address the Next Hop Server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** command in interface configuration mode. 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 or 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 the IP address of that Next Hop Server, the Next Hop Server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

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 Next Hop Resolution Protocol (NHRP) server-only mode, use the **ip nhrp server-only** command in interface configuration mode. 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 Switched Virtual Circuit (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 the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ip nhrp trigger-svc** command in interface configuration mode. 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 an NHRP request.

ip nhrp use

To configure the software so that Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ip nhrp use** command in interface configuration mode. 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

usage-count 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 send 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 sent immediately. Configuring the *usage-count* argument causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 10.0.0.1 and one 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 is 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 five packets are sent to the first destination and five 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 resends its request for the second destination.

```
ip nhrp use 5
```

Related Commands

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

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command in interface configuration mode. 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 redirects

To enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ip redirects

no ip redirects

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.

Usage Guidelines Previously, if the Hot Standby Router Protocol (HSRP) was configured on an interface, ICMP redirect messages were disabled by default for the interface. With Cisco IOS Release 12.1(3)T, ICMP redirect messages are enabled by default if HSRP is configured.

Examples The following example enables the sending of ICMP redirect messages on Ethernet interface 0:

```
interface ethernet 0
 ip redirects
```

Related Commands	Command	Description
	ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
	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 routing

To enable IP routing, use the **ip routing** command in global configuration mode. 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 To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging 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 slb dfp

To configure the Dynamic Feedback Protocol (DFP) and supply an optional password, use the **ip slb dfp** command in global configuration mode. To remove the DFP configuration, use the **no** form of this command.

```
ip slb dfp [password password [timeout]]
```

```
no ip slb dfp
```

Syntax Description

password	(Optional) Specifies a password for MD5 authentication.
<i>password</i>	(Optional) Password value for MD5 authentication. This password must match the password configured on the host agent.
<i>timeout</i>	(Optional) Delay period (in seconds) during which both the old password and the new password are accepted. The default value is 180 seconds.

Defaults

The password timeout default is 180 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The optional password, if configured, must match the password configured on the host agent.

The *timeout* option allows you to change the password without stopping messages between the DFP agent and its manager. The default value is 180 seconds.

During the timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the agent sends and receives packets only with the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. This setting allows enough time for you to update the password on all agents and servers before the timeout expires. It also prevents mismatches between agents and servers that have begun running the new password and agents, and servers on which you have not yet changed the old password.

Examples

The following example configures DFP, sets the password to flounder, configures a timeout period of 60 seconds, and changes to DFP configuration mode:

```
ip slb dfp flounder 60
```

Related Commands

Command	Description
agent	Configures a DFP agent.

ip slb serverfarm

To identify a server farm and enter SLB server farm configuration mode, use the **ip slb serverfarm** command in global configuration mode. To remove the server farm from the IOS SLB configuration, use the **no** form of this command.

ip slb serverfarm *serverfarm-name*

no ip slb serverfarm *serverfarm-name*

Syntax Description

<i>serverfarm-name</i>	Character string used to identify the server farm. The character string is limited to 15 characters.
------------------------	--

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

The following example identifies a server farm named PUBLIC:

```
ip slb serverfarm PUBLIC
```

Related Commands

Command	Description
real	Identifies a real server.

ip slb vserver

To identify a virtual server and enter SLB virtual server configuration mode, use the **ip slb vserver** command in global configuration mode. To remove a virtual server from the IOS SLB configuration, use the **no** form of this command.

ip slb vserver *virtserver-name*

no ip slb vserver *virtserver-name*

Syntax Description	<i>virtserver-name</i>	Character string used to identify the virtual server. The character string is limited to 15 characters.
---------------------------	------------------------	---

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

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

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

Examples The following example identifies a virtual server named PUBLIC_HTTP:

```
ip slb vserver PUBLIC_HTTP
```

Related Commands	Command	Description
	serverfarm	Associates a real server farm with a virtual server.
	show ip slb vservers	Displays information about the virtual servers.

ip source-route

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

ip source-route

no ip source-route

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 handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands	Command	Description
	ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
	ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** command in global configuration mode. 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 0 subnets. Subnetting with a subnet address of 0 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 tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp chunk-size *characters*

no ip tcp chunk-size

Syntax Description	<i>characters</i>	Maximum number of characters that Telnet or rlogin can read in one read instruction. The default value is 0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.
---------------------------	-------------------	--

Defaults	0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.
-----------------	--

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

Command History	Release	Modification
	9.1	This command was introduced.

Usage Guidelines	It is unlikely you will need to change the default value.
-------------------------	---

Examples	The following example sets the maximum TCP read size to 64,000 bytes: <pre>ip tcp chunk-size 64000</pre>
-----------------	---

ip tcp compression-connections

To specify the total number of TCP header compression connections that can exist on an interface, use the **ip tcp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections *number*

Syntax Description

<i>number</i>	Number of TCP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).
---------------	---

Defaults

The default number is 32 connections.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay, PPP, and High-Level Data Link Control (HDLC) encapsulation, the maximum number of compression connections increased to 256. For Frame Relay, the maximum value is fixed, not configurable.

Usage Guidelines

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.



Note

Both ends of the serial connection must use the same number of cache entries.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.

Command	Description
ip tcp header-compression	Enables TCP header compression.
show ip rtp header-compression	Displays RTP header compression statistics.

ip tcp header-compression

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

ip tcp header-compression [passive]

no ip tcp header-compression [passive]

Syntax Description	passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the passive keyword, the Cisco IOS software compresses all traffic.
---------------------------	----------------	--

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

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This condition means that fast interfaces like T1 can overload the router. Consider the traffic characteristics of your network before using this command.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands	Command	Description
	ip tcp header-compression	Specifies the total number of header compression connections that can exist on an interface.

ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss** command in global configuration mode. To disable the configuration of the MSS, use the **no** form of this command.

ip tcp mss *mss-value*

no ip tcp mss *mss-value*

Syntax Description

<i>mss-value</i>	Maximum segment size for TCP connections in bytes. The range is from 68 to 10000.
------------------	---

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(05)S	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.

Usage Guidelines

If this command is not enabled, the MSS value of 536 bytes is used if the destination is not on a LAN, otherwise the MSS value is 1460 for a local destination.

For connections originating from a router, the specified value is used directly as an MSS option in the synchronize (SYN) segment. For connections terminating on a router, the value is used only if the incoming SYN segment has an MSS option value higher than the configured value. Otherwise the incoming value is used as the MSS option in the SYN/acknowledge (ACK) segment.



Note

The **ip tcp mss** command interacts with the **ip tcp path-mtu-discovery** command and not the **ip tcp header-compression** command. The **ip tcp path-mtu-discovery** command changes the default MSS to 1460 even for non-local nodes.

Examples

The following example sets the MSS value at 250:

```
ip tcp mss 250
```

Related Commands

Command	Description
ip tcp header-compression	Specifies the total number of header compression connections that can exist on an interface.

ip tcp path-mtu-discovery

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

```
ip tcp path-mtu-discovery [age-timer {minutes | infinite}]
```

```
no ip tcp path-mtu-discovery [age-timer {minutes | infinite}]
```

Syntax Description

age-timer <i>minutes</i>	(Optional) Time interval (in minutes) after which TCP re-estimates the path MTU with a larger maximum segment size (MSS). The maximum is 30 minutes; the default is 10 minutes.
age-timer infinite	(Optional) Turns off the age timer.

Defaults

Disabled. If enabled, the default *minutes* value is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The age-timer and infinite keywords were added.

Usage Guidelines

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection. It is described in RFC 1191. Existing connections are not affected when this feature is turned on or off.

Customers using TCP connections to move bulk data between systems on distinct subnets would benefit most by enabling this feature.

The age timer is a time interval for how often TCP re-estimates the path MTU with a larger MSS. When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You can turn off the age timer by setting it to infinite.

Examples

The following example enables Path MTU Discovery:

```
ip tcp path-mtu-discovery
```

ip tcp queuemax

To alter the maximum TCP outgoing queue per connection, use the **ip tcp queuemax** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp queuemax *packets*

no ip tcp queuemax

Syntax Description	<i>packets</i>	Outgoing queue size of TCP packets. The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.
---------------------------	----------------	--

Defaults	The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.
-----------------	--

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Changing the default value changes the 5 segments, not the 20 segments.
-------------------------	---

Examples	The following example sets the maximum TCP outgoing queue to 10 packets: <pre>ip tcp queuemax 10</pre>
-----------------	---

ip tcp selective-ack

To enable TCP selective acknowledgment, use the **ip tcp selective-ack** command in global configuration mode. To disable TCP selective acknowledgment, use the **no** form of this command.

ip tcp selective-ack

no ip tcp selective-ack

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round-trip time. An aggressive sender could resend packets early, but such re-sent segments might have already been received.

The TCP selective acknowledgment mechanism helps overcome these limitations. The receiving TCP returns selective acknowledgment packets to the sender, informing the sender about data that has been received. The sender can then resend only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when a multiple number of packets drop from a TCP window. There is no performance impact when the feature is enabled but not used.

This command becomes effective only on new TCP connections opened after the feature is enabled.

This feature must be disabled if you want TCP header compression. You might disable this feature if you have severe TCP problems.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

Examples

The following example enables the router to send and receive TCP selective acknowledgments:

```
ip tcp selective-ack
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

ip tcp synwait-time

To set a period of time the Cisco IOS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** command in global configuration mode. To restore the default time, use the **no** form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Syntax Description	<i>seconds</i>	Time (in seconds) the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.
---------------------------	----------------	---

Defaults	The default time is 30 seconds.
-----------------	---------------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	In versions previous to Cisco IOS software Release 10.0, the system would wait a fixed 30 seconds when attempting to establish a TCP connection. If your network contains public switched telephone network (PSTN) dial-on-demand routing (DDR), the call setup time may exceed 30 seconds. This amount of time is not sufficient in networks that have dialup asynchronous connections because it will affect your ability to Telnet over the link (from the router) if the link must be brought up. If you have this type of network, you may want to set this value to the UNIX value of 75.
-------------------------	---

Because this is a host parameter, it does not pertain to traffic going *through* the router, just for traffic originated *at* this device. Because UNIX has a fixed 75-second timeout, hosts are unlikely to experience this problem.

Examples	The following example configures the Cisco IOS software to continue attempting to establish a TCP connection for 180 seconds:
-----------------	---

```
ip tcp synwait-time 180
```

ip tcp timestamp

To enable TCP time stamp, use the **ip tcp timestamp** command in global configuration mode. To disable TCP time stamp, use the **no** form of this command.

ip tcp timestamp

no ip tcp timestamp

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2 F	This command was introduced.

Usage Guidelines TCP time stamp improves round-trip time estimates. Refer to RFC 1323 for more detailed information on TCP time stamp.

The TCP time stamp must be disabled if you want to use TCP header compression.

Examples The following example enables the router to send TCP time stamps:

```
ip tcp timestamp
```

Related Commands	Command	Description
	ip tcp header-compression	Enables TCP header compression.

ip tcp window-size

To alter the TCP window size, use the **ip tcp window-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip tcp window-size *bytes*

no ip tcp window-size

Syntax Description

<i>bytes</i>	Window size (in bytes). An integer from 0 to 1,073,741,823. The default value is 4128 bytes. Window scaling is enabled when the window size is greater than 65,535 bytes.
--------------	---

Defaults

The default window size is 4128 bytes when window scaling is not enabled. If only one neighbor is configured for the window scaling extension, the default window size is 65,535 bytes.

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.
12.2(8)T	Default window size and maximum window scaling factor were increased.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

To enable window scaling to support Long Fat Networks (LFNs), the TCP window size must be more than 65,535 bytes. The remote side of the link also needs to be configured to support window scaling. If both sides are not configured with window scaling, the default maximum value of 65,535 bytes is applied.

The scale factor is automatically calculated based on the window-size you configure. You cannot directly configure the scale factor.

Examples

The following example sets the TCP window size to 1000 bytes:

```
ip tcp window-size 1000
```

ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode. 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 High Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and 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 Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered, which 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 the address of Ethernet 0:

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

ip unreachable

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachable** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip unreachable

no ip unreachable

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

Usage Guidelines If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects all types of ICMP unreachable messages.

Examples The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ip unreachable
```

ip vrf (tracking)

To configure a VPN routing and forwarding (VRF) table, use the **ip vrf** command in tracking configuration mode. To remove a VRF routing table, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description	<i>vrf-name</i>	Name assigned to a VRF.
--------------------	-----------------	-------------------------

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

Command Modes	Tracking configuration
---------------	------------------------

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

Usage Guidelines	This command is available for all IP route tracked objects that are tracked by the track ip route global configuration command. Use this command to track a route belonging to a specific VPN.
------------------	---

Examples	In the following example, the route associated with a VRF named VRF1 will be tracked:
----------	---

```
track 1 ip route 10.16.0.0/16 reachability
delay down 30
ip vrf VRF1
```

Related Commands	Command	Description
	track ip route	Tracks the state of an IP route and enters tracking configuration mode.



Note

The **ip wccp {web-cache | service-number} group-list** command syntax resembles the **ip wccp {web-cache | service-number} group-listen** command, but these are entirely different commands. Note that the **ip wccp group-listen** command is an interface configuration command, used to configure an interface to listen for multicast notifications from a cache cluster. See the description of the **ip wccp group-listen** command in this chapter for more information.

ip wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group and deallocate space, use the **no** form of this command.

```
ip wccp { web-cache | service-number } [service-list service-access-list] [mode { open | closed }]
  [group-address multicast-address] [redirect-list access-list] [group-list access-list]
  [password [0-7] password]
```

```
no ip wccp { web-cache | service-number } [service-list service-access-list] [mode { open | closed }]
  [group-address multicast-address] [redirect-list access-list] [group-list access-list]
  [password [0-7] password]
```

Syntax Description

web-cache	Specifies the web-cache service (WCCP version 1 and version 2). Note Web cache counts as one service. The maximum number of services, including those assigned with the <i>service-number</i> argument, are 256.
<i>service-number</i>	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the web-cache keyword. Note If Cisco Cache Engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
service-list <i>service-access-list</i>	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
open	(Optional) Identifies the service as open. This is the default service mode.
closed	(Optional) Identifies the service as closed.
group-address <i>multicast-address</i>	(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which web cache should receive redirected messages.
redirect-list <i>access-list</i>	(Optional) Access list that controls traffic redirected to this service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list <i>access-list</i>	(Optional) Access list that determines which web caches are allowed to participate in the service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password [0-7] <i>password</i>	(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be any value between 0 and 7 (inclusive), with 0 specifying not yet encrypted and 7 for proprietary. The <i>password</i> argument can be up to eight characters in length.

Defaults

WCCP services are not enabled on the router.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.1	This command replaced the ip wccp enable , ip wccp redirect-list , and ip wccp group-list commands.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.3(14)T	The maximum value for the <i>service-number</i> argument was increased to 254.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	The service-list <i>service-access-list</i> keyword and argument pair and the mode open and mode closed keywords were added.

Usage Guidelines WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching should be enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command should be specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

This command instructs a router to enable or disable the support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

ip wccp { web-cache | service-number } group-address multicast-address

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all “Here I Am” messages are responded to with a unicast reply.

ip wccp { **web-cache** | *service-number* } **redirect-list** *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- User Datagram Protocol (UDP) (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic will prevent the web caches from ever seeing the packets that are intercepted.

ip wccp { **web-cache** | *service-number* } **group-list** *access-list*

This option instructs the router to use an access list to control the web caches allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.



Note

The **ip wccp** { **web-cache** | *service-number* } **group-list** command syntax resembles the **ip wccp** { **web-cache** | *service-number* } **group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ip wccp group-listen** command in the [Cisco IOS IP Application Services Command Reference](#), Release 12.4T.

ip wccp { **web-cache** | *service-number* } **password** *password*

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

ip wccp *service-number* **service-list** *service-access-list* **mode closed**

In applications where the interception and redirection of WCCP packet flows to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, it is necessary to block packet flows for the application when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client
10.1.1.13
```

When there is a conflict in service list definitions, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
ip multicast-routing
ip wccp 99 group-address 239.0.0.0
interface ethernet 0
 ip wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
access-list 100 deny ip any host 10.168.196.51
access-list 100 permit ip any any
ip wccp web-cache redirect-list 100
interface ethernet 0
 ip wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
ip wccp web-cache
ip wccp check acl outbound
interface fastethernet0/0
 ip access-group 10 out
 ip wccp web-cache redirect out
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

The following example shows how to configure a closed WCCP service:

```
ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP you wish to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp enable

The **ip wccp enable** has been replaced by the **ip wccp** command. See the description of the **ip wccp** command in this chapter for more information.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for the Web Cache Communication Protocol (WCCP) feature, use the **ip wccp group-listen** command in interface configuration mode. To remove control of the reception of IP multicast packets for the WCCP feature, use the **no** form of this command.

ip wccp {web-cache | service-number} group-listen

no ip wccp {web-cache | service-number} group-listen

Syntax Description	web-cache	Directs the router to send packets to the web cache service.
	<i>service-number</i>	The identification number of the cache engine service group being controlled by a router. The number can be from 0 to 99.

Defaults This command is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- The IP multicast address for use by the WCCP Service Group must be configured.
- The interfaces on which the router wishes to receive the IP multicast address to be configured with the **ip wccp {web-cache | service-number} group-listen** interface configuration command.

Examples In the following example, a user enables the multicast packets for a web cache with a multicast address of 224.1.1.100.

```
router# configure terminal
router(config)# ip wccp web-cache group-address 244.1.1.100
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache group listen
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a WCCP cache engine service group.
	ip wccp <service> redirect	Enables WCCP redirection on an interface.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp {web-cache | service-number} redirect {in | out}
```

```
no ip wccp {web-cache | service-number} redirect {in | out}
```

Syntax Description

web-cache	Enables the web-cache service.
<i>service-number</i>	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Defaults

Redirection checking on the interface is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(11)S	The in keyword was added.
12.1(3)T	The in keyword was added.
12.2(17d)SXB	Support for this command on the Cisco 7600 series router Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 720.
12.2(18)SXF	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.



Tips

Be careful not to confuse the **ip wccp redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.



Note

This command has the potential to affect the **ip wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the “exclude in” command will be overridden. The opposite is also true: configuring the “exclude in” command will override the “redirect in” command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when fast/CEF switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ip address 10.21.21.1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ip nat outside
Router(config-if)# ip inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP statistics.

ip wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ip wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description

This command has no arguments or keywords.

Defaults

Redirection exclusion is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

This configuration command instructs the interface to exclude inbound packets from any redirection check that may occur at the outbound interface. Note that the command is global to all the services and should be applied to any inbound interface that you wish to exclude from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the internet as well as allow for the use of the WCCPv2 Packet Return feature.

Examples

In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
Router(config)# interface ethernet 0
Router(config-if)# ip wccp redirect exclude in
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a cache engine service group.
	ip wccp redirect out	Configures an interface to enable a the ability of a router to verify that appropriate packets are being redirected to a cache engine.

ip wccp redirect-list

This command is now documented as part of the **ip wccp** { **web-cache** | *service-number* } command. See the description of the **ip wccp** command in this book for more information.

ip wccp version

To specify which version of Web Cache Communication Protocol (WCCP) you wish to configure on your router, use the **ip wccp version** command in global configuration mode.

ip wccp version {1 | 2}

Syntax Description

1	Web Cache Communication Protocol Version 1 (WCCPv1).
2	Web Cache Communication Protocol Version 2 (WCCPv2).

Defaults

WCCPv2

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
router# show ip wccp
% WCCP version 2 is not enabled
router# configure terminal
router(config)# ip wccp version 1
router(config)# end
router# show ip wccp
% WCCP version 1 is not enabled
```

ip web-cache redirect

The **ip web-cache redirect** interface configuration command has been replaced by the **ip wccp redirect** interface configuration command. The **ip web-cache redirect** command is no longer supported. See the description of the **ip wccp redirect** command in this book for more information.