

ip nat source through iterate-ip-addrs

- ip nat settings gatekeeper-size, on page 3
- ip nat settings high-performance, on page 4
- ip nat settings nonpatdrop, on page 6
- ip nat source, on page 7
- ip nat stateful id, on page 9
- ip nat switchover replication http, on page 11
- ip nat translation, on page 12
- ip nat translation (timeout), on page 13
- ip nat translation max-entries, on page 16
- ip nat translation max-entries cpu, on page 19
- ip netmask-format, on page 20
- ip nhrp authentication, on page 21
- ip nhrp group, on page 22
- ip nhrp holdtime, on page 24
- ip nhrp interest, on page 25
- ip nhrp map, on page 26
- ip nhrp map group, on page 28
- ip nhrp map multicast, on page 30
- ip nhrp map multicast dynamic, on page 31
- ip nhrp max-send, on page 33
- ip nhrp multicast, on page 35
- ip nhrp network-id, on page 36
- ip nhrp nhs, on page 37
- ip nhrp record, on page 40
- ip nhrp redirect, on page 41
- ip nhrp registration, on page 43
- ip nhrp registration no-unique, on page 45
- ip nhrp responder, on page 46
- ip nhrp resolution refresh base, on page 47
- ip nhrp send-routed, on page 49
- ip nhrp server-only, on page 50
- ip nhrp shortcut, on page 51
- ip nhrp trigger-svc, on page 52

- ip nhrp use, on page 53
- ip options, on page 55
- ip proxy-arp, on page 57
- ip route, on page 58
- ip route vrf, on page 63
- ip routing, on page 67
- ip source binding, on page 68
- ip source-route, on page 70
- ip sticky-arp (global configuration), on page 71
- ip sticky-arp (interface configuration), on page 73
- ip subnet-zero, on page 74
- ip unnumbered, on page 75
- IP Unnumbered Ethernet Polling Support, on page 78
- ip verify source vlan dhcp-snooping, on page 79
- ipv4-prefix, on page 80
- ipv6 address autoconfig, on page 81
- ipv6 address dhcp, on page 83
- ipv6 address dhcp client request, on page 84
- ipv6 dhcp binding track ppp, on page 85
- ipv6 dhcp client information refresh minimum, on page 86
- ipv6 dhcp client pd, on page 87
- ipv6 dhcp database, on page 89
- ipv6 dhcp debug redundancy, on page 91
- ipv6 dhcp framed password, on page 92
- ipv6 dhcp guard attach-policy, on page 93
- ipv6 dhcp guard policy, on page 95
- ipv6 dhcp iana-route-add, on page 96
- ipv6 dhcp iapd-route-add, on page 97
- **ipv6 dhcp-ldra** , on page 98
- ipv6 dhcp-ldra attach-policy, on page 99
- ipv6 dhcp ldra attach-policy (VLAN), on page 101
- ipv6 dhcp ping packets, on page 102
- ipv6 dhcp pool, on page 103
- ipv6 dhcp relay destination, on page 106
- ipv6 dhcp-relay source-interface, on page 109
- ipv6 dhcp-relay bulk-lease, on page 110
- ipv6 dhcp-relay option vpn, on page 111
- ipv6 dhcp-relay show bindings, on page 112
- ipv6 dhcp-relay source-interface, on page 113
- ipv6 dhcp server, on page 114
- ipv6 dhcp server vrf enable, on page 116
- ipv6 inspect tcp finwait-time, on page 117
- ipv6 nd managed-config-flag, on page 118
- ipv6 nd other-config-flag, on page 120
- ipv6-prefix, on page 122
- iterate-ip-addrs, on page 123

ip nat settings gatekeeper-size

To modify gatekeeper cache size, use the **ip nat settings gatekeeper-size** command. This command allows allocating gatekeeper cache in the power of two based on the number of entries configured.

ip nat settings gatekeeper-size *number of entries*
no ip nat settings gatekeeper *number of entries*

Syntax Description

number of entries	Number of entries that can be stored in gatekeeper cache. Each entry has source and destination ip address of the packet.

Command Default

If gatekeeper service is enabled, gatekeeper cache size is allocated with default value. The default value is based on the platform.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1a	This command was introduced in 3.13 MCP release. Maximum entries allowed for gatekeeper was 256k. In 17.11 release, maximum number of entries supported has been extended to 1 million entries.

Usage Guidelines

When a device is sending both NAT mode and non-NAT mode traffic, increase gatekeeper cache size to skip nat processing for non-NAT mode traffic.

Examples

The following example shows how to enable the **ip nat settings gatekeeper size** command on the device.

```
Router(config)#ip nat settings gatekeeper-size 1048576
Router(config)#end
```

Related Commands

Command	Description
ip nat service gatekeeper	Enables gatekeeper service to tag non-NAT mode traffic to skip NAT processing.

ip nat settings high-performance

To allow high connection setup rate for non-ALG NAT traffic, use the **ip nat settings high- performance** command. This command only supports pool overload configuration. To disable high connection set up rate, use the **no** form of this command.

ip nat settings high-performance
no ip nat settings high-performance

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

CGN operating mode and Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.2 Amsterdam	This command was introduced for ASR 1000 platform.

Usage Guidelines

Before enabling this command ensure that the following prerequisites are met:

- The paired address pooling is disabled using **no ip nat settings pap** command
- The end-point mapping is not configurable
- The application level gateways are disabled
- Reload the router after using this command

Examples

The following example shows how to enable the **ip nat settings high performance** command on the device.

```
!
Router(config)# ip nat settings high-performance
Router(config)# exit
Router(config-if)# reload
```

Examples

The following example shows how to verify if **ip nat settings high performance** command is working.

```
!
Router# show platform hardware qfp active feature nat datapath basecfg
```

Related Commands

Command	Description
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip nat settings nonpatdrop

This command enables the behavior related to non-PATable NAT translations. To configure this setting, use the **ip nat settings nonpatdrop** command in global configuration mode. To disable or remove this setting, use the **no** form of this command.

ip nat settings nonpatdrop
no ip nat settings nonpatdrop

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
16.4.1	This command was introduced.

Usage Guidelines

Using the **ip nat settings nonpatdrop** command, the router drops packets that cause Non-Pattable NAT translation attempts, which are traffic types without port numbers, instead of creating one-to-one bindings. This helps conserve NAT pool addresses and prevents address exhaustion from such traffic.

Examples

The following example shows how to enable the **ip nat settings nonpatdrop** command to control the behavior of non-PATable NAT translations:

```
Router(config)# ip nat settings nonpatdrop
```

ip nat source

To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode.

Dynamic NAT
ip nat source {**list** {*access-list-numberaccess-list-name*} **interface** *type number* | **pool** *name*} [**overload** | **vrf** *name*]

Static NAT
ip nat source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]
no ip nat source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Port Static NAT

Network Static NAT
ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]
no ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Syntax Description

list *access - list-number*	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 *access - list-name*	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.
interface *type*	Specifies the interface type for the global address.
interface *number*	Specifies the interface number for the global address.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static *local-ip*	Sets up a single static translation. The *local-ip* argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from the RFC 1918, or obsolete.
local-port	Sets the local TCP/UDP port in a range from 1 to 65535.

static *global-ip*	Sets up a single static translation. The *local-ip* argument establishes the globally unique IP address of an inside host as it appears to the outside network.
global-port	Sets the global TCP/UDP port in the range from 1 to 65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits as alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
esp *local-ip*	Establishes IPSec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network *local-network*	Specified the local subnet translation.
global-network	Specifies the global subnet translation.
mask	Establishes the IP network mask to be used with subnet translations.

Command Modes

Global Configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to configure a virtual interface without inside or outside specification for the global address:

```
ip nat source list 1 pool NAT vrf bank overload
ip nat source list 1 pool NAT vrf park overload
ip nat source static 192.168.123.1 192.168.125.10 vrf services
```

Related Commands

Command	Description
ip nat enable	Configures an interface connecting VPNs and the Internet for NAT translation.
ip nat pool	Defines a pool of IP addresses for Network Address Translation.

ip nat stateful id

To designate the members of a translation group, use the **ip nat stateful id** command in global configuration mode. To disable the members of a translation group or reset default values, use the **no** form of this command.

no ip nat stateful id *id-number*

Syntax Description

id-number	Unique number given to each router in the stateful translation group.
redundancy *name*	Establishes Hot Standby Routing Protocol (HSRP) as the method of redundancy.
mapping-id *map-number*	Specifies whether or not the local Stateful (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
protocol	(Optional) Enables the HSRP UDP default to be changed to TCP.
tcp	(Optional) Establishes the Transmission Control Protocol.
udp	(Optional) Establishes the User Datagram Protocol.
as -queuing	(Optional) Enables asymmetric routing during queuing for HSRP to be disabled.
disable	(Optional) Disables asymmetric routing during queuing in HSRP mode.
enable	(Optional) Enables asymmetric routing during queuing in HSRP mode.
primary i*p-address-primary*	Manually establishes redundancy for the primary router.
backup i*p-address-backup*	Manually establishes redundancy for the backup router.
peer *ip-address-peer*	Specifies the IP address of the peer router in the translation group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(3)	The **protocol** and **as-queuing**keywords were added.
12.4(4)T	This command was intregrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command has two forms: HSRP stateful NAT and manual stateful NAT. 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.

In HSRP mode, the default TCP can be changed to UDP by using the optional **protocol udp** keywords with the **redundancy keyword**.

To disable the queuing during asymmetric routing in HSRP mode, use the optional **as-queuing disable** keywords with the **redundancy** keyword.

Examples

The following example shows how to configure SNAT with HSRP:

```
!
standby delay minimum 30 reload 60
standby 1 ip 10.1.1.1
standby 1 name SNATHSRP
standby 1 preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
as-queuing disable
protocol udp
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

The following example shows how to manually configure SNAT:

```
ip nat stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
ip nat stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

Related Commands

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

ip nat switchover replication http

To enable replication of HTTP sessions during a switchover, use the **ip nat switchover replication http** command in global configuration mode. To disable replication of HTTP sessions during a switchover, use the **no** form of this command.

ip nat switchover replication http *port-number*
no ip nat switchover replication http

Syntax Description

port-number	HTTP port number. Valid values are from 1 to 65535.

Command Default

Replication of HTTP sessions during a switchover is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.0	This command was introduced.

Usage Guidelines

By default, NAT high availability (inter- and intra-box) does not replicate HTTP sessions to the standby router. Use the **ip nat switchover replication http** command to replicate HTTP sessions on the standby router during a switchover. Replication refers to the backing up of HTTP sessions on the standby router. HTTP sessions are usually short-lived connections and to reduce the high availability (HA) traffic between active and standby routers, backing up of HTTP sessions are avoided. The **ip nat switchover replication http** command enables you to control the replication of HTTP sessions based on your requirements.

Examples

The following example shows how to enable replication of HTTP sessions during a switchover:

```
Router(config)# ip nat switchover redundancy http 65
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for an interface is subject to NAT.

ip nat translation

The **ip nat translation** command is replaced by the **ip nat translation**(timeout) and **ip nat translation max-entries** commands. See these commands for more information.

ip nat translation (timeout)

To change the Network Address Translation (NAT) timeout, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** | **udp**} *port-number* | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**} {*seconds* | **never**}
no ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** | **udp**} *port-number* | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**}

Syntax Description

arp-ping-timeout	Specifies that the timeout value applies to the Address Resolution Protocol (ARP) ping.
dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. The default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
tcp	Specifies TCP.
udp	Specifies UDP.
port-number	Port number for TCP or UDP. The range is from 1 to 65535.
pptp-timeout	Specifies that the timeout value applies to NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86,400 seconds (24 hours).
routemap-entry-timeout	Specifies that the timeout applies for a half entry created by a route map.
syn-timeout	Specifies that the timeout value applies to TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
timeout	Specifies that the timeout value applies to dynamic translations, except for overload translations. The default is 86,400 seconds (24 hours).

udp-timeout	Specifies that the timeout value applies to the UDP port. The default is 300 seconds (5 minutes).
seconds	Number of seconds after which the specified port translation times out.
never	Specifies that port translation will not time out.

Command Default

NAT translation timeouts are enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	This command was modified. The **arp-ping-timeout** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **routemap-entry-timeout**, **tcp**, **udp**, and *port-number* keywords and arguments were added.

Usage Guidelines

When port translation is configured, each entry contains more information about the traffic that is using the translation, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless a TCP Reset (RST) or a Finish (FIN) bit is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example shows how to configure the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
Router# configure terminal
Router(config)# 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; enables NAT logging; or enables static IP address support.
ip nat inside destination	Enables NAT of a globally unique host address to multiple inside host addresses.
ip nat inside source	Enables NAT of the inside source address.

Command	Description
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	Specifies a port other than the default port for NAT.
ip nat translation max-entries	Limits the size of a NAT table to a specified maximum.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat translation max-entries

To limit the size of a Network Address Translation (NAT) table to a specified maximum, use the **ip nat translation max-entries** command in global configuration mode. To remove a specified limit, use the **no** form of this command.

ip nat translation max-entries {**all-host** | **all-vrf** | **host** *ip-address* | **list** {*list-namelist-number*} | **redundancy** *redundancy-id number-of-entries* | **vrf** *name*} *number*
no ip nat translation max-entries {**all-host** | **all-vrf** | **host** *ip-address* | **list** {*list-namelist-number*} | **redundancy** *redundancy-id number-of-entries* | **vrf** *name*} *number*

Syntax Description

all-host	Constrains each host by the specified number of NAT entries.
all-vrf	Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
host	Constrains an IP address by the specified NAT limit.
ip-address	IP address subject to the NAT limit.
list	Constrains an access control list (ACL) by the specified NAT limit.
list-name	ACL name subject to the NAT limit.
list-number	ACL number subject to the NAT limit.
redundancy	Specifies the NAT entries for redundancy groups (RGs).
redundancy-id	Redundancy ID. The range is from 1 to 2.
number-of-entries	Number of NAT entries. The range is from 1 to 2147483647.
vrf	Constrains an individual VRF instance by the specified NAT limit.
name	Name of the VRF instance subject to the NAT limit.
number	Maximum number of allowed NAT entries. The range is from 1 to 2147483647.



Note Note: On an ASR 1000 platform, if you are configuring Box-to-Box redundancy using the redundancy keyword, the limit set on the NAT table is ignored. Therefore, to enforce the limit, use the **ip nat translation max-entries** command without the redundancy keyword. For example: **ip nat translation max-entries** *number*command.

Command Default

No maximum size is specified for the NAT table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword-argument pair was removed from Cisco 7600 series routers.
Cisco IOS XE Release 3.5S	This command was modified. The **redundancy** keyword and *redundancy-id* and *number-of-entries* arguments were added.
15.2(3)T	This command was modified. The order of precedence of the keywords was changed. For more information, see the "Usage Guidelines" section.

Usage Guidelines

Before you configure a NAT rate limit, you must first classify the current NAT usage and determine the sources of requests for NAT translations. If a specific host, an ACL, or a VRF instance is generating an unexpectedly high number of NAT requests, the host may be the source of a virus or worm attack.

Once you have identified the source of excessive NAT requests, you can set a NAT rate limit that constrains a specific host, an ACL, or a VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.



Note When using the **no** form of the **ip nat translation max-entries** command, you must specify the type of NAT rate limit that you want to remove and its value. For more information about how to display the current NAT rate limit settings, see the **show ip nat statistics** command.

Prior to Cisco IOS Release 15.2(3)T, the order of precedence of keywords in the **ip nat translation max-entries** command is **vrf**, **all-vrf**, **host**, **all-host**, and **list**. For example, if you have configured the **ip nat translation max-entries list 50 2** and **ip nat translation max-entries all-host 10** commands in your NAT configuration, the **ip nat translation max-entries all-host 10** command overrides the **ip nat translation max-entries list 50 2** command, making the **ip nat translation max-entries list** command redundant. In Cisco IOS Release 15.2(3)T and later releases, the order of precedence of keywords is **vrf**, **all-vrf**, **host**, **list**, and **all-host**.

Examples

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
ip nat translation max-entries 300
```

Setting NAT Limits for VRF Instances

The following example shows how to limit each VRF instance to 200 NAT entries:

```
ip nat translation max-entries all-vrf 200
```

The following example shows how to limit the VRF instance named vrf1 to 150 NAT entries:

```
ip nat translation max-entries vrf vrf1 150
```

The following example shows how to limit the VRF instance named vrf2 to 225 NAT entries, but limit all other VRF instances to 100 NAT entries each:

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

Setting NAT Limits for ACLs

The following example shows how to limit the ACL named vrf3 to 100 NAT entries:

```
ip nat translation max-entries list vrf3 100
```

Setting NAT Limits for an IP Address

The following example shows how to limit the host at IP address 10.0.0.1 to 300 NAT entries:

```
ip nat translation max-entries host 10.0.0.1 300
```

Related Commands

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

ip nat translation max-entries cpu

To configure the CPU utilization threshold for limiting the number of NAT translations, use the **ip nat translation max-entries cpu** command in global configuration mode.

To remove the CPU utilization threshold, use the **no** form of this command.

ip nat translation max-entries cpu *desired-percentage*
no ip nat translation max-entries cpu *desired-percentage*

Note The feature enabled by the **ip nat translation max-entries cpu** command is supported in Autonomous mode and is compatible with both classic NAT and CGN operational modes, but not in SD-WAN environments.

Syntax Description

cpu *desired-percentage*	Specifies the maximum CPU utilization threshold as a percentage of total CPU resources that can be used for processing NAT translations.

Command Default

By default, there is no CPU utilization threshold set for NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

Set this threshold based on the average CPU load and performance requirements of your network. Monitor CPU utilization following threshold configuration; persistent high usage with no new translations may indicate a problem that requires Cisco support.

If the **clear ip nat translation** command is issued and the CPU utilization remains high (87 to 90 percent), without the gatekeeper command being configured, it is crucial to investigate and address the underlying issue to prevent service degradation.

This feature, enabled via the above command, requires cooperation with the NAT gatekeeper for proper management of NAT resources and synchronization.

Examples

The following example sets the CPU utilization threshold for NAT translations to 70%:

```
Device# configure terminal
Device(config)# ip nat translation max-entries cpu 70
```

ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format**command inline 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

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

Command Default

Netmasks are displayed in dotted-decimal format.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 10.108.11.0 255.255.255.0.

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 10.108.11.0 0XFFFFFF00.

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 10.108.11.0/24.

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 ininterface 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

string	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.

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All routers configured with NHRP within one logical nonbroadcast multiaccess (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 group



Note The command **ip nhrp group** has been deprecated and is not in use. Use the command **nhrp group** instead of **ip nhrp group**.

To configure a Next Hop Resolution Protocol (NHRP) group on a spoke, use the **ip nhrp group**command in interface configuration mode. To remove an NHRP group, use the **no** form of this command.

ip nhrp group *group-name*
no ip nhrp group *group-name*

Syntax Description

group-name	Specifies an NHRP group name.

Command Default

No NHRP groups are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.4(1)T / 3.11S	This command was replaced with *nhrp group* and hidden.
16.6.5, 16.8.1	This hidden command was removed, manual migration to new syntax required before or after upgrade.

Usage Guidelines

After you create an NHRP group on a spoke, you use the **ip nhrp map group**command to map the group to a QoS policy map.

Examples

The following example shows how to create two NHRP groups named small and large.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp group small
Router(config-if)# ip nhrp group large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.

Command	Description
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

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 ininterface 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

seconds	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. **Note** The recommended NHRP hold time value ranges from 300 to 600 seconds. Although a higher value can be used when required, we recommend that you do not use a value less than 300 seconds; and if used, it should be used with extreme caution.

Command Default

7200 seconds (2 hours)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 ininterface 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

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

Command Default

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command with the **access-list** command to control which IP packets trigger NHRP requests.

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

Examples

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

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

Related Commands

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

ip nhrp map

To statically configure the IP-to-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* [**preference** *pref*]
no ip nhrp map *ip-address nbma-address* [**preference** *pref*]

Syntax Description

ip-address	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	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.
preference *pref*	(Optional) Assigns a preference for the IP-to-NBMA address mapping. The preference must be in the range 1 to 255.

Command Default

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)T	This command was modified. NBMA address was modified to support IPv6 address.
Cisco IOS XE Release 16.8.1	This command was modified. Option to assign a preference for IP-to-NBMA address mapping was added.

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 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured to be 192.0.0.1 and the NBMA address for 10.0.1.3 is 192.2.7.8.

```
interface tunnel 0
```

```
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.1.3
ip nhrp map 10.0.0.1 192.0.0.1 preference 3
ip nhrp map 10.0.1.3 192.2.7.8 preference 9
```

Related Commands

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

ip nhrp map group



Note The command **ip nhrp map group** has been deprecated and is not in use. Use the command **nhrp map group** instead of **ip nhrp map group**.

To associate a Next Hop Resolution Protocol (NHRP) group to a QoS policy map, use the **ip nhrp map group**command in interface configuration mode. To remove an association, use the **no** form of this command.

ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*
no ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

Syntax Description

group-name	Specifies an NHRP group name.
qos-policy-map-name	Specifies a QoS policy map name.

Command Default

No mappings are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.4(1)T / 3.11S	This command was replaced with *nhrp map group* and hidden.
16.6.5, 16.8.1	This hidden command was removed, manual migration to new syntax required before or after upgrade.

Usage Guidelines

The command allows a QoS policy in the output direction only.

Examples

The following example shows how to map two NHRP groups named small and large to two QoS policy maps named qos-small and qos-large respectively.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp map group small service-policy output qos-small
Router(config-if)# ip nhrp map group large service-policy output qos-large
```

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.

Command	Description
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

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

nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using.

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)T	This command was modified. NBMA address was modified to support IPv6 address.

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 10.0.0.1 and 10.0.0.2. Addresses 10.0.0.1 and 10.0.0.2 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 10.0.0.1
 ip nhrp map multicast 10.0.0.2
```

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 or to clear dynamic entries, 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.

Command Default

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M3	This command was modified to enable the clearing of all dynamic entries in the multicast table by using the **no** form of this command.

Usage Guidelines

Use this command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IPSecurity (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.

You can clear all dynamic entries in the multicast table by using the **no** form of this command.

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
 bandwith 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 10.17.0.1 255.255.255.0
```

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** *seconds*
no ip nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
every *seconds*	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Command Default

pkt-count : 100 packets*seconds:*10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 *seconds*argument.

- This command needs to take into consideratin the number of spoke routers being handled by this hub and how often they send NHRP registration requests. To support this load you would need:

Number of spokes / registration timeout * *Max-send-interval*

- • Example

500 spokes with 100 second Registration timeout

Max send value = 500/100*10 = 50

- The Maximum number of spoke-spoke tunnels that are expected to be up at any one time across the whole DMVPN network.

spoke-spoke tunnels/NHRP holdtime * Max-send-interval

This would cover spoke-spoke tunnel creation and the refreshing of spoke-spoke tunnels that are used for longer periods of time.

- • Example

2000 spoke-spoke tunnels with 250 second hold timeout

Max send value = 2000/250*10 = 80

Then add these together and multiply this by 1.5 - 2.0 to give a buffer.

- • Example

Max send = (50 + 80) * 2 = 260

- The max-send-interval can be used to keep the long term average number of NHRP messages allowed to be sent constant, but allow greater peaks.
    - Example

400 messages in 10 seconds

In this case it could peak at approximately 200 messages in the first second of the 10 second interval, but still keep to a 40 messages per second average over the 10 second interval.

4000 messages in 100 seconds

In this case it could peak at approximately 2000 messages in the first second of the 100 second interval, but it would still be held to 40 messages per second average over the 100 second interval. In the second case it could handle a higher peak rate, but risk a longer period of time when no messages can be sent if it used up its quota for the interval.

By default, the maximum rate at which the software sends NHRP packets is five packets per 10 seconds. The software maintains a per-interface quota of NHRP packets (whether generated locally or forwarded) that can be sent.

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 multicast

To configure multicast batch size and batch interval, use the **ip nhrp multicast** command in interface configuration mode. To remove the multicast batch size and batch interval configuration, use the **no** form of this command.

ip nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

no ip nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

Syntax Description

batch-size *num*	Specifies the batch size of multicast replication.
batch-interval *milliseconds*	Specifies the interval for batch multicast replication.

Command Default

The default multicast batch-size is 250. The default multicast batch-interval is 10 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
IOS XE Release 16.8.1	Command introduced.

Usage Guidelines

By replacing **ip** in the command name with **ipv6**, you can set the multicast batch size and interval for IPv6 traffic.

Example

The following example shows the multicast batch-size configured to 12 and the batch-interval configured to 10 milliseconds for a tunnel interface.

```
interface tunnel0
 ip nhrp multicast batch-size 12 batch-interval 10
```

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id**command ininterface 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

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

Command Default

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases
ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]
no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Cisco IOS Release 15.1(2)T and Later Releases
ip nhrp nhs {*nhs-address* [**nbma** {*nbma-addressFQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-addressFQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}
no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-addressFQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-addressFQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

Syntax Description

nhs-address	Address of the next-hop server being specified.
net-address	(Optional) IP address of a network served by the next-hop server.
netmask	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.
max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Command Default

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The *net-address* and *mask* arguments were removed and the **nbma**, *nbma-address*, *FQDN-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.
15.2(1)T	This command was modified. The NBMA address was modified to support IPv6 address.

Usage Guidelines

Use the **ip nhrp nhs** 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.

When the **ip nhrp nhs dynamic** command is configured on a DMVPN tunnel and the **shut** command is issued to the tunnel interface, the crypto socket does not receive shut message, thereby not bringing up a DMVPN session with the hub.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address*argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

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

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.

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 redirect

To enable Next Hop Resolution Protocol (NHRP) redirect, use the **ip nhrp redirect**command in interface configuration mode. To remove the NHRP redirect, use the **no** form of this command.

ip nhrp redirect [**timeout** *seconds*]
no ip nhrp redirect [**timeout** *seconds*]

Syntax Description

timeout *seconds*	Indicates the interval, in seconds, that the NHRP redirects are sent for the same nonbroadcast multiaccess (NBMA) source and destination combination. The range is from 2 to 30 seconds.

Command Default

NHRP redirect is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NHRP redirect message is an indication that the current path to the destination is not optimal. The receiver of the message should find a better path to the destination.

This command generates an NHRP redirect traffic indication message if the incoming and outgoing interface is part of the same DMVPN network. The NHRP shortcut switching feature depends on receiving the NHRP redirect message. NHRP shortcut switching does not trigger an NHRP resolution request on its own. It triggers an NHRP resolution request only after receiving an NHRP redirect message.

Most of the traffic would follow a spoke-hub-spoke path. NHRP redirect is generally required to be configured on all the DMVPN nodes in the event the traffic follows a spoke-spoke-hub-spoke path, which is unlikely the case.

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to enable NHRP redirects on the interface:

```
Router> enable

Router# configure terminal
Router(config)# interface Tunnel0
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
```

```
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp shortcut	Enables NHRP shortcut switching.

ip nhrp registration

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** command in interface configuration mode. To reenable this functionality, use the **no** form of this command.

ip nhrp registration [**timeout** *seconds* | **no-unique** | **req-def-map** [**include-label**]]
no ip nhrp registration [**timeout** *seconds* | **no-unique** | **req-def-map** [**include-label**]]

Syntax Description

timeout *seconds*	(Optional) Time between periodic registration messages. • *seconds* --Number of seconds. The range is from 1 through the value of the NHRP hold timer. • If the **timeout** keyword is not specified, NHRP registration messages are sent every number of seconds equal to 1/3 the value of the NHRP hold timer.
no-unique	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.
req-def-map	(Optional) Enables the client to request default maps in registration.
include-label	(Optional) Enables the client to request default maps with labels in registration.

Command Default

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced.
12.3(7.2)	The **timeout** keyword and *seconds*argument were added. In addition, effective with Cisco IOS Release 12.3(7.2), this command replaced the **ip nhrp registration no-unique** command.
12.3(7)T	The **timeout** keyword and *seconds*argument were integrated into Cisco IOS Release 12.3(7)T. In addition, the replacement of the **ip nhrp registration no-unique** command with this command was integrated into Cisco IOS Release 12.3(7)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 16.10.1	The **req-def-map** keyword was added.
Cisco IOS XE Release 17.11.1a	The **include-label** keyword was added.

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** command and **no-unique** keyword, the unique flag is not set, and the NHS can override the old registration information.

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

By configuring the **ip nhrp registration** command and the **req-def-map** keyword, the NHRP client requests for default map from the server via registration message.

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
```

The following example shows that the registration timeout is set to 120 seconds, and the delay is set to 5 seconds:

```
interface FastEthernet 0/0
 ip nhrp registration 120
```

The following example configures the client to enable requesting default maps in registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration req-def-map
```

The following example configures the client to enable requesting default maps with labels in registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration req-def-map include-label
```

Related Commands

Command	Description
ip nhrp holdtime	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses

ip nhrp registration no-unique

The **ip nhrp registration no-unique** command is replaced by the **ip nhrp registration command.**See the **ip nhrp registration**command for more information.

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 ininterface configuration mode. To remove the designation, use the **no** form of this command.

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

Syntax Description

interface-type	Interface type whose primary IP address is used when a next-hop server complies with a Responder Address option (for example, **serial or tunnel**).
interface-number	Interface number whose primary IP address is used when a next-hop server complies with a Responder Address option.

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 resolution refresh base

The default NHRP resolution requests follow the routed path to the destination spoke (exit point out the DMVPN cloud). For the first resolution request, this routed path is via the hub(s) all the way to the destination spoke. Owing to the on-demand route created as a result of the resolution process, for a resolution request sent for refreshing on-demand spoke-spoke routes and tunnels the routed path is the direct path between the spokes. This revalidates the direct spoke-spoke path like a keepalive and also reduces the load on the hub.

You can use this command to make the requests follow the base routed path via the hub(s), and do not take the on-demand path/route that was learnt for the prefix/next hop.

ip nhrp resolution refresh base *number*
no ip nhrp resolution refresh base

Syntax Description

refresh	Displays resolution refresh-related configuration options.
base	Configures the base routed path for routing resolution requests for refresh. This excludes the on-demand/shortcut routed path for routing resolution requests for refreshes.
number	(Optional) Specifies which refresh goes through the base path.

Command Default

The default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 17.4 Release	The **refresh** and **base** keywords were introduced to the **ip nhrp resolution refresh base** command.

Usage Guidelines

Use **ip nhrp resolution refresh base** *number* on the tunnel interface on the spoke when it is intended that the resolution requests follow the base routed path via the hub(s) and don't take the on-demand path/route that was learnt for the prefix/next hop. When configured, it should be configured symmetrically at both ends, else, it leads to asymmetric behavior.

Examples

The following example displays what the *number* denotes:

- When the value is n=1, every refresh goes through the base path.
- When the value is n=2, every second refresh goes through the base path, while other values still follow the default behaviour.

```
ip nhrp resolution refresh base 1
```

Related Commands

Command	Description
ip nhrp send-routed	This command is enabled by default and causes NHRP control packets to be sent over the routed path.

Command	Description
no ip nhrp send-routed	This command causes NHRP control packets to be sent over the routed path to the destination/next hop. This is enabled by default.

ip nhrp send-routed

To forward the resolution requests via the routed path, use **ip nhrp send-routed** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip nhrp send-routed
no ip nhrp send-routed

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
16.9	This command was introduced.

Usage Guidelines

With **ip nhrp send-routed** configured, the control packets take the routed path instead of nhs priority path. Without send-routed, the nhs priority configuration takes effect. The path taken by the control packets can be verfied using **show ip nhrp traffic** command.

For all non-registration packets, the first NHRP resolution request takes the route installed by the IGP initially and then is forwarded along the routed path, for subsequent requests. The routed path can be the NHRP route or NHOs.

If the routed path fails for some reasons, tunnel falls back to the NHS path.

By replacing **ip** in the command name with **ipv6**, you can forward the resolution requests via the routed path for IPv6 traffic.

Examples

The following is an example of tunnel interface when the tunnel interface is disabled:

```
interface Tunnel1
ip address 192.168.10.10 255.255.255.0
no ip redirects
ip nhrp authentication C!sco123
ip nhrp network-id 1
ip nhrp nhs 192.168.10.1 nbma 172.16.10.1 multicast
no ip nhrp send-routed
tunnel source GigabitEthernet2
tunnel mode gre multipoint
end
```

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 ininterface 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.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0	The **non-caching** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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:

```
ip nhrp server-only
```

ip nhrp shortcut

To enable Next Hop Resolution Protocol (NHRP) shortcut switching, use the **ip nhrp shortcut**command in interface configuration mode. To remove shortcut switching from NHRP, use the **no** form of this command.

ip nhrp shortcut
no ip nhrp shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

The NHRP shortcut switching is enabled in Cisco IOS XE Everest 16.6.2 and Cisco IOS 15.7(2)M releases and later. Prior to these releases, this command was disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Everest Release 16.6.2 and Cisco IOS Release 15.7(2)M	By default, NHRP shortcut switching was enabled.

Usage Guidelines

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to configure an NHRP shortcut on an interface:

```
Router> enable

Router# configure terminal
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp redirect	Enables NHRP redirect.

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 ininterface 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

trigger-threshold	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.
teardown-threshold	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.

Command Default

trigger-threshold : 1 kbps

teardown-threshold : 0 kbps

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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**commandininterface 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.

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 options

To drop or ignore IP options packets that are sent to the router, use the **ip options**command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

ip options {**drop** | **ignore**}
no ip options {**drop** | **ignore**}

Syntax Description

drop	Router drops all IP options packets that it receives.
ignore	Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet--just ignored.) **Note** This option is not available on the Cisco 10000 series router.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(19)	This command was integrated into Cisco IOS Release 12.3(19).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 for the PRE3.

Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and you configure the ignore mode, the ignore mode overrides the drop mode.

Cisco 10720 Internet Router

The **ip options ignore** command is not supported. Only drop mode (the **ip options drop** command) is supported.

Cisco 10000 Series Router

This command is only available on the PRE3. The PRE2 does not support this command.

The **ip options ignore** command is not supported. The router supports only the **ip options drop** command.

Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
 ignore modes.
end
```

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.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration.

Examples

The following example enables proxy ARP on Ethernet interface 0:

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

Related Commands

Command	Description
ip arp proxy disable	Globally disables proxy ARP.

ip route

To establish static routes, use the **ip route** command in global configuration mode. Toremove static routes, use the **no**form of this command.

ip route [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
no ip route [**vrf** *vrf-name*] *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.

Release	Modification
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network**(DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static**command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>
router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
```

RIP and EIGRP do not redistribute the route with the following **ip route**command because of the split horizon algorithm:

```
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

- EIGRP redistributes the route with both of the following commands:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static**command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers

each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3) with a static route to prevent routes from passing through an unintended interface.



Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**,displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
```

```
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config
 | include ip route
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route vrf

To establish static routes for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf**command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]
no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

Supported Static Route Configurations

When you configure static routes in a Multiprotocol Label Switching (MPLS) or MPLS VPN environment, note that some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS releases 12.*x* T, 12.*x* M, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1 ip route** *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf**commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  • **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1* **ip route vrf** *vrf-name destination-prefix ma sk interface2 next-hop2*

The following **ip route vrf**commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet gateway.

- • **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
  • **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address* (This command is supported when the next hop and interface are in the core.)

The following **ip route**commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1 ip route** *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global ip route vrf** *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1 ip route vrf** *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf**command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (EBGP) multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1 ip route** *destination-prefix mask* **interface2 nexthop2**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
redistribute static	Redistributes routes from another routing domain into the specified domain.

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.

Command Default

IP routing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.

Disabling IP routing is not allowed if you are running Cisco IOS Release 12.2SX on a Catalyst 6000 platform. The workaround is to not assign an IP address to the SVI.

Examples

The following example enables IP routing:

```
Router# configure terminal
Router(config
)
# ip routing
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *type mod/port*

Syntax Description

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *type*	Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

Examples

This example shows how to add a static IP source binding entry:

```
Router(config)#
ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface gigabitethernet5/3
```

This example shows how to delete a static IP source binding entry:

```
Router(config)#
no ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface gigabitethernet5/3
```

Related Commands

Command	Description
ip verify source vlan dhcp snooping	Enables or disables the per 12-port IP source guard.
show ip source binding	Displays the IP source bindings configured on the system.

Command	Description
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

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.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 sticky-arp (global configuration)

To enable sticky ARP, use the **ip sticky-arp** command in global configuration mode. To disable sticky ARP, use the **no** form of this command.

ip sticky-arp
no ip sticky-arp

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to support all Layer 3 interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In releases prior to Release 12.2(18)SXF, sticky ARP was supported on PVLAN interfaces only.

You can enter the **ip sticky-arp (interface configuration)**command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

Examples

This example shows how to enable sticky ARP:

```
Router(config) ip sticky-arp
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (interface configuration)	Enables sticky ARP on an interface.
show arp	Displays the ARP table.

ip sticky-arp (interface configuration)

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

ip sticky-arp [**ignore**]
no ip sticky-arp [**ignore**]

Syntax Description

ignore	(Optional) Overwrites the **ip sticky-arp**(global configuration) command.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter this command on any Layer 3 interface.

You can enter the **ip sticky-arp ignore** command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.

Examples

This example shows how to enable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
 ignore
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (global configuration)	Enables sticky ARP.
show arp	Displays the ARP table.

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.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 unnumbered

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

ip unnumbered *type number* [**poll**]
no ip unnumbered [*type number*]

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (**?**) online help function.
poll	(Optional) Enables IP connected host polling.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was made available on the Supervisor Engine 720.
12.2(18)SXF	This command was modified to support Ethernet physical interfaces and switched virtual interfaces (SVIs).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers..
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY. The **poll** keyword was added.

Usage Guidelines

When an 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.

The following restrictions are applicable for this command:

- This command is not supported on Cisco 7600 Series Routers that are configured with a Supervisor Engine 32.
- 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.
- This interface configuration command cannot be used 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.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface that you specify using 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 must configure the serial interfaces as unnumbered. This configuration allows you to comply 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 that you specified as unnumbered, any routing protocol that is running across the serial line must not advertise subnet information.

Examples

The following example shows how to assign the address of Ethernet 0 to the first serial interface:

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# interface serial 0
Device(config-if)# ip unnumbered ethernet 0
```

The following example shows how to configure Ethernet VLAN subinterface 3/0.2 as an IP unnumbered subinterface:

```
Device(config)# interface ethernet 3/0.2
Device(config-subif)# encapsulation dot1q 200
Device(config-subif)# ip unnumbered ethernet 3/1
```

The following example shows how to configure Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 as IP unnumbered subinterfaces:

```
Device(config)# interface range fastethernet5/1.1 - fastethernet5/1.4
Device(config-if-range)# ip unnumbered ethernet 3/1
```

The following example shows how to enable polling on a Gigabit Ethernet interface:

```
Device(config)# interface loopback0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
```

```
!
Device(config-if)# ip unnumbered gigabitethernet 3/1
Device(config-if)# ip unnumbered loopback0 poll
```

IP Unnumbered Ethernet Polling Support

ip verify source vlan dhcp-snooping

To enable Layer 2 IP source guard, use the **ip verify source vlan dhcp-snooping** command in the service instance mode. Use the **no** form of this command to disable Layer 2 IP source guard.

ip verify source vlan dhcp-snooping [**port-security**]
no ip verify source vlan dhcp-snooping [**port-security**]

Syntax Description

port-security	Enables IP/MAC mode and applies both IP and MAC filtering.

Command Default

Layer 2 IP source guard is disabled.

Command Modes

Service instance (config-if-srv)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **port-security**keyword was added.

Usage Guidelines

The **ip verify source vlan dhcp-snooping** command enables VLANs only on the configured service instance (EVC) and looks for DHCP snooping matches only for the configured bridge domain VLAN.

Examples

This example shows how to enable Layer 2 IP source guard on an interface:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation dot1q 71
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)#  bridge-domain 10
```

Related Commands

Command	Description
service instance ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

ipv4-prefix

To configure an IPv4 prefix for a Network Address Translation 64 (NAT64) mapping of address and ports translation (MAP-T) basic mapping rule, use the **ipv4-prefix** command in NAT64 MAP-T BMR configuration mode. To remove the IPv4 prefix, use the **no** form of this command.

ipv4-prefix *ipv4-prefix/prefix-length*
no ipv4-prefix *ipv4-prefix/prefix-length*

Syntax Description

ipv4-prefix/prefix-length	IPv4 prefix in dotted decimal and the length of the IPv4 prefix. The prefix-length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure an IPv4 prefix for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# ipv4-prefix 198.51.100.1/32
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig [**default**]
no ipv6 address autoconfig

Syntax Description

default	(Optional) If a default device is selected on this interface, the **default** keyword causes a default route to be installed using that default device. The **default** keyword can be specified only on one interface.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address autoconfig** command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [**rapid-commit**]
no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

ipv6 address dhcp client request vendor
no ipv6 address dhcp client request vendor

Syntax Description

vendor	Requests the vendor-specific options.

Command Default

IPv6 clients are not configured to request an option from DHCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **ipv6 address dhcp client request vendor** command to request a vendor-specific option. When this command is enabled, the IPv6 client can request a vendor-specific option only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has acquired an IPv6 address, the IPv6 client cannot request a vendor-specific option until the next time the client acquires an IPv6 address from DHCP.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp client request vendor
```

Related Commands

Command	Description
ipv6 address dhcp	Acquires an IPv6 address on an interface from the DHCPv6 server.

ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the **ipv6 dhcp binding track ppp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

Syntax Description

This command has no arguments or keywords.

Command Default

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp binding track ppp** command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using this command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator clears the binding.

Examples

The following example shows how to release the prefix bindings associated with the PPP:

```
Router(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable Dynamic Host Configuration Protocol (DHCP) for IPv6 client information refresh time on a specified interface, use the **ipv6 dhcp client information refresh minimum**command in interface configuration mode. To remove the configured refresh time, use the **no** form of this command.

ipv6 dhcp client information refresh minimum *seconds*
no ipv6 dhcp client information refresh minimum *seconds*

Syntax Description

seconds	The refresh time, in seconds. The minimum value that can be used is 600 seconds.

Command Default

The default is 86,400 seconds (24 hours).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The **ipv6 dhcp client information refresh minimum**command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

Examples

The following example configures an upper limit of 2 hours:

```
ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
no ipv6 dhcp client pd

Syntax Description

prefix-name	IPv6 general prefix name.
hint	An IPv6 prefix sent as a hint.
ipv6-prefix	IPv6 general prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation.

Command Default

Prefix delegation is disabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Enabling the **ipv6 dhcp client pd**command starts the DHCP for IPv6 client process if this process is not yet running.

The **ipv6 dhcp client pd**command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the *ipv6-prefix*argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The **hint** keyword with the *ipv6-prefix* argument enables the configuration of an IPv6 prefix that will be included in DHCP for IPv6 solicit and request messages sent by the DHCP for IPv6 client on the interface as a hint to prefix-delegating routers. Multiple prefixes can be configured by issuing the **ipv6 dhcp client pd hint***ipv6-prefix* command multiple times. The new prefixes will not overwrite old ones.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Examples

The following example enables prefix delegation:

```
Router(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Router(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

Related Commands

Command	Description
clear ipv6 dhcp client	Restarts the DHCP for IPv6 client on an interface.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds. Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or administrators enable the clear ipv6 dhcp binding command. These bindings are maintained in RAM and can be saved to permanent storage using the *agent* argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are terminated. By default, the DHCP for IPv6 server waits 300 seconds before terminating a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

ipv6 dhcp debug redundancy

To display debugging output for IPv6 DHCP high availability (HA) processing, use the **ipv6 dhcp debug redundancy**command in privileged EXEC mode. To disable debugging output, use the no form of this command.

ipv6 dhcp debug redundancy
no ipv6 dhcp debug redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp debug redundancy** command to display stateful switchover (SSO) state transitions and errors.

Examples

The following example enables IPv6 DHCP redundancy debugging:

```
Router# ipv6 dhcp debug redundancy
```

ipv6 dhcp framed password

To assign a framed prefix when using a RADIUS server, use the **ipv6 dhcp framed password**command in interface configuration mode. To remove the framed prefix, use the **no** form of this command.

ipv6 dhcp framed password *password*
no ipv6 dhcp framed password

Syntax Description

password	Password to be used with the RADIUS server.

Command Default

No framed prefix is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The ipv6 dhcp framed password command enables a user to request a framed prefix of a RADIUS server. When a PPPoE client requests a prefix from a network using the framed-prefix system, the RADIUS server should assign an address. However, the RADIUS server is configured to receive a password. Because the client does not send a password, the RADIUS server does not send a framed prefix.



Note Ordinarily, the **ipv6 dhcp framed password** command will not need to be used because a client will have been authenticated as part of PPP session establishment.

Examples

The following example shows how to configure a password to be used with the RADIUS server:

```
Router(config-if)# ipv6 dhcp framed password password1
```

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode
ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]
no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]

Syntax Available In VLAN Configuration Mode
ipv6 dhcp guard attach-policy [*policy-name*]
no ipv6 dhcp guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
vlan-id	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default

No DHCPv6 guard policy is attached.

Command Modes

Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy [*policy-name*]
no ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default

No DHCPv6 guard policy name is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to define a DHCPv6 guard policy name:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

Related Commands

Command	Description
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp iana-route-add

To add routes for individually assigned IPv6 addresses on a relay or server, use the **ipv6 dhcp iana-route-add** command in global configuration mode. To disable route addition for individually assigned IPv6 addresses on a relay or server, use the **no** form of the command.

ipv6 dhcp iana-route-add
no ipv6 dhcp iana-route-add

Syntax Description

This command has no arguments or keywords.

Command Default

Route addition for individually assigned IPv6 addresses on a relay or server is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The **ipv6 dhcp iana-route-add** command is disabled by default and has to be enabled if route addition is required. Route addition for Internet Assigned Numbers Authority (IANA) is possible if the client is connected to the relay or server through unnumbered interfaces, and if route addition is enabled with the help of this command.

Examples

The following example shows how to enable route addition for individually assigned IPv6 addresses:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp iana-route-add
```

ipv6 dhcp iapd-route-add

To enable route addition by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay and server for the delegated prefix, use the **ipv6 dhcp iapd-route-add** command in global configuration mode. To disable route addition, use the **no** form of the command.

ipv6 dhcp iapd-route-add
no ipv6 dhcp iapd-route-add

Syntax Description

This command has no arguments or keywords.

Command Default

DHCPv6 relay and DHCPv6 server add routes for delegated prefixes by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The DHCPv6 relay and the DHCPv6 server add routes for delegated prefixes by default. The presence of this command on a router does not mean that routes will be added on that router. When you configure the command, routes for delegated prefixes will only be added on the first Layer 3 relay and server.

Examples

The following example shows how to enable the DHCPv6 relay and server to add routes for a delegated prefix:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp iapd-route-add
```

ipv6 dhcp-ldra

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on an access node, use the **ipv6 dhcp-ldra** command in global configuration mode. To disable the LDRA functionality, use the **no** form of this command.

ipv6 dhcp-ldra {enable | disable}
no ipv6 dhcp-ldra {enable | disable}

Syntax Description

enable	Enables LDRA functionality on an access node.
disable	Disables LDRA functionality on an access node.

Command Default

By default, LDRA functionality is not enabled on an access node.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You must configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on a VLAN or an access node (such as a Digital Subscriber Link Access Multiplexer [DSLAM] or an Ethernet switch) interface.

Example

The following example shows how to enable the LDRA functionality:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# exit
```

Note In the above example, Device denotes an access node.

Related Commands

Command	Description
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

ipv6 dhcp-ldra attach-policy

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a port or interface, use the **ipv6 dhcp-ldra attach-policy** command in interface configuration mode. To disable LDRA functionality on an interface or port, use the **no** form of this command.

ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}
no ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.
client-facing-disable	Disables LDRA functionality on an interface or port.
server-facing	Specifies an interface or port as server facing.

Command Default

By default, LDRA functionality is not enabled on an interface or port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on an interface or port.

The **ipv6 dhcp-ldra attach-policy** command enables LDRA functionality on a specific interface or port. Instead of configuring LDRA individually on all the client-facing interfaces or ports individually, use the **ipv6 dhcp ldra attach-policy** command to configure LDRA on an entire VLAN.

Example

The following example shows how to enable LDRA functionality on an interface and specify it as server facing:

```
Device>enable
Device#configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface ethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.

ipv6 dhcp ldra attach-policy (VLAN)

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a VLAN, use the **ipv6 dhcp ldra attach-policy** command in VLAN configuration mode. To disable LDRA functionality on a VLAN, use the **no** form of this command.

ipv6 dhcp ldra attach-policy {client-facing-trusted | client-facing-untrusted}
no ipv6 dhcp ldra attach-policy {client-facing-trusted | client-facing-untrusted}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.

Command Default

By default, the LDRA functionality is not enabled on a VLAN.

Command Modes

VLAN configuration (config-vlan-config)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on a VLAN.

In a typical deployment, a majority of the interfaces or ports on a device are client facing. Instead of configuring LDRA individually on all the client facing interfaces and ports, use the **ipv6 dhcp ldra attach-policy** command to configure LDRA on the entire VLAN. As a result, all the ports or interfaces associated with the VLAN will be configured as client facing.

Example

The following example shows how to enable LDRA functionality on a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# vlan configuration 5
Device(config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted
Device(config-vlan-config)# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

Syntax Description

number	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]

Cisco CMTS Routers

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address***source-address*]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address** *source-address*]

Syntax Description

ipv6-address	Relay destination address. There are two types of relay destination address: • Link-scoped unicast or multicast IPv6 address. A user must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type interface-number	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) associated with the relay destination IPv6 address.
global	(Optional) Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a VRF.
link-address *link-address*	(Optional) Specifies the DHCPv6 link address. The link-address must be an IPv6 globally scoped address configured on the network interface where the DHCPv6 relay is operational.
source-address *source-address*	(Optional) Specifies the Cisco CMTS network interface source address. The source-address can be any IPv6 global-scoped address on the router.

Command Default

The relay function is disabled, and there is no relay destination on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added. The **global** keyword was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
12.2(33)SCE5	This command was integrated into Cisco IOS Release 12.2(33)SCE5. The **link-address** and **source-address** keywords were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

In Cisco CMTS, if you change one or more parameters of this command, you have to disable the command using the no form, and execute the command again with changed parameters.

The default behavior (when **no source-address**, **link-address**, and **no output interface** commands are provisioned in the **ipv6 dhcp relay destination** command) of the new functionality is to copy the Cisco IOS SAS-computed source address to the link-address of the DHCPv6 relay-forward message.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789 ethernet 4/3
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type *interface-number*	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode. To remove the bulk-lease query configuration, use the **no** form of this command.

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]
no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

Command Default

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the **ipv6 dhcp-relay bulk-lease**command with the **disable** keyword.

Examples

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

Related Commands

Command	Description

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the ipv6 dhcp-relay option vpn command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp-relay show bindings

To enable the DHCPv6 relay agent to list prefix delegation (PD) bindings, use the **ipv6 dhcp-relay show bindings**command in global configuration mode. To disable PD binding tracking, use the no form of this command.

ipv6 dhcp-relay show bindings
no ipv6 dhcp-relay show bindings

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **ipv6 dhcp-relay show bindings** command lists the PD bindings that the relay agent is tracking. The command lists the bindings in the relay's radix tree, lists DHCPv6 relay routes, and prints each entry's prefix and length, client identity association identification (IAID), and lifetime. <<Any more information here?>>

Examples

The following example enables the DHCPv6 relay agent to list PD bindings: <<OK?>>:

```
Router# ipv6 dhcp-relay show bindings
```

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type *interface-number*	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a

relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable**command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCPv6 server VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on the router.

Examples

The following example enables the DHCPv6 server VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp server option vpn
```

ipv6 inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a FIN-exchange, use the **ipv6 inspect tcp finwait-timeip inspect tcp finwait-time**command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ipv6 inspect tcp finwait-time *seconds*
no ipv6 inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483.

Command Default

Command Modes

Global configuration (config)

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

ipv6 nd managed-config-flag

To set the "managed address configuration flag" in IPv6 router advertisements, use the **ipv6 nd managed-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "managed address configuration flag" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Setting the "managed address configuration flag" flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

The following example configures the "managed address configuration flag" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
ipv6 nd prefix-advertisement	Configures which IPv6 prefixes are included in IPv6 router advertisements

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

The "other stateful configuration" flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The setting of the "other stateful configuration" flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.



Note If the "managed address configuration" flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the "other stateful configuration" flag.

Examples

The following example configures the "other stateful configuration" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6-prefix

To configure an IPv6 address for a Network Address Translation 64 (NAT64) mapping of address and ports translation (MAP-T) basic mapping rule, use the **ipv6-prefix** command in NAT64 MAP-T BMR configuration mode. To remove the IPv6 address, use the **no** form of this command.

ipv6-prefix *ipv6-prefix/prefix-length*
no ipv6-prefix

Syntax Description

ipv6-prefix/prefix-length	The IPv6 address assigned to the interface and the length of the IPv6 prefix. The prefix-length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS Release 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure an IPv6 address for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# ipv6-prefix 2001:0DB8:0:1::/64
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

iterate-ip-addrs

To display the interface descriptor blocks (IDBs) that are visited by the IP iterators, use the **iterate-ip-addrs** command in privileged EXEC mode.

iterate-ip-addrs *target-ip-address mask* [**secondary**] [**time-only**]

Syntax Description

target-ip-address	Target IP address.
mask	Target IP address mask.
secondary	(Optional) Displays the secondary addresses.
time-only	(Optional) Displays only the time measurements of all macros.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated in a release earlier than Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output of the **iterate-ip-addrs secondary** command:

```
Router# iterate-ip-addrs 10.0.0.1 255.0.0.0 secondary
target = 10.0.0.1, mask = 255.0.0.0, sec = TRUE
  interface            primary address     tableid
  -------------------- ------------------  ----------
FOR_SWIDBS_WITH_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=0 microsec
FOR_SWIDBS_ON_IPSUBNET(idb, tbl, target & mask, mask, sec, cref) visits
  Gi6/2                     10.4.9.87/24  0x00000000
        ExecTime=1 microsec
FOR_SWIDBS_WITH_IPNETADDR(idb, tbl, target, mask, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_WHOSE_SUBNET_HAS_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_SWIDBS(idb, tbl, cref) visits
  Gi6/2                     10.4.9.87/24  0x00000000
  EO0/0                    192.0.2.51/8   0x00000FFF
  Gi1/1                     10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
  interface            address             tableid
  -------------------- ------------------  ----------
FOR_ENTRIES_ON_IPSUBNET(addr, tbl, target & mask, mask, cref) visits
  Gi6/2                     10.4.9.87/24  0x00000000
        ExecTime=2 microsec
FOR_NUMBERED_ENTRIES(addr, tbl, cref) visits
  Gi6/2                     10.4.9.87/24  0x00000000
  EO0/0                    192.0.2.51/8   0x00000FFF
  Gi1/1                     10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
```

```
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES(addr, tbl, cref) visits
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES_WITH_IPADDR(addr, tbl, target, cref) visits
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALIAS
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits INTERFACE
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALL
  Gi6/2                      10.4.9.87/24  0x00000000
  EO0/0                     192.0.2.51/8   0x00000FFF
  Gi1/1                      10.1.1.1/24   0x00000000
  Vl1                    192.0.2.1/24  0x00000000
        ExecTime=2 microsec
Summary
Macro No. 0     ExecTime=0 microsec
Macro No. 1     ExecTime=1 microsec
Macro No. 2     ExecTime=1 microsec
Macro No. 3     ExecTime=1 microsec
Macro No. 4     ExecTime=2 microsec
Macro No. 5     ExecTime=2 microsec
Macro No. 6     ExecTime=2 microsec
Macro No. 7     ExecTime=2 microsec
Macro No. 8     ExecTime=1 microsec
Macro No. 9     ExecTime=1 microsec
Macro No. 10    ExecTime=1 microsec
Macro No. 11    ExecTime=2 microsec
Router# iterate-ip-addrs 10.0.0.1 255.0.0.0 secondary time-only

target = 10.0.0.1, mask = 255.0.0.0, sec = TRUE
  interface            primary address     tableid
  -------------------- ------------------  ----------
FOR_SWIDBS_WITH_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_ON_IPSUBNET(idb, tbl, target & mask, mask, sec, cref) visits
        ExecTime=2 microsec
FOR_SWIDBS_WITH_IPNETADDR(idb, tbl, target, mask, sec, cref) visits
        ExecTime=1 microsec
FOR_SWIDBS_WHOSE_SUBNET_HAS_IPADDR(idb, tbl, target, sec, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_SWIDBS(idb, tbl, cref) visits
        ExecTime=2 microsec
interface            address             tableid
  -------------------- ------------------  ----------
FOR_ENTRIES_ON_IPSUBNET(addr, tbl, target & mask, mask, cref) visits
        ExecTime=1 microsec
FOR_NUMBERED_ENTRIES(addr, tbl, cref) visits
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES(addr, tbl, cref) visits
        ExecTime=2 microsec
FOR_ALL_IPADDR_ENTRIES_WITH_IPADDR(addr, tbl, target, cref) visits
        ExecTime=0 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALIAS
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits INTERFACE
```

```
        ExecTime=1 microsec
FOR_TYPED_IPADDR_ENTRIES(addr, tbl, cref) visits ALL
        ExecTime=2 microsec
Summary
Macro No. 0     ExecTime=1 microsec
Macro No. 1     ExecTime=2 microsec
Macro No. 2     ExecTime=1 microsec
Macro No. 3     ExecTime=1 microsec
Macro No. 4     ExecTime=2 microsec
Macro No. 5     ExecTime=1 microsec
Macro No. 6     ExecTime=2 microsec
Macro No. 7     ExecTime=2 microsec
Macro No. 8     ExecTime=0 microsec
Macro No. 9     ExecTime=1 microsec
Macro No. 10    ExecTime=1 microsec
Macro No. 11    ExecTime=2 microsec
```