IP Addressing Services Commands

clear ip nhrp

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

clear ip nhrp[{**vrf** {*vrf-name* | **global**}}] [{*dest-ip-address* [{*dest-mask*}] | **tunnel** *number* | **counters** [{**interface tunnel** *number*}] | **stats** [{**tunnel** *number* [{**vrf** {*vrf-name* | **global**}}]}]}]

Syntax Description

vrf	(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the VRF address family to which the command is applied.
global	(Optional) Specifies the global VRF instance.
dest-ip-address	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.
dest-mask	(Optional) Destination network mask.
counters	(Optional) Clears the NHRP counters.
interface	(Optional) Clears the NHRP mapping entries for all interfaces.
tunnel *number*	(Optional) Removes the specified interface from the NHRP cache.
stats	(Optional) Clears all IPv4 statistic information for all interfaces.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The **clear ip nhrp** command does not clear any static (configured) IP-to-NBMA address mappings from the NHRP cache.

Examples

The following example shows how to clear all dynamic entries from the NHRP cache for an interface:

```
Switch# clear ip nhrp
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

debug nhrp

To enable Next Hop Resolution Protocol (NHRP) debugging, use the **debug nhrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } | **umatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate**}]
no debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } **unmatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate** }]

Syntax Description

attribute	(Optional) Enables NHRP attribute debugging operations.
cache	(Optional) Enables NHRP cache debugging operations.
condition	(Optional) Enables NHRP conditional debugging operations.
interface tunnel *number*	(Optional) Enables debugging operations for the tunnel interface.
nbma	(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.
ipv4-nbma-address	(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.
nbma-name	(Optional) NBMA network name.
IPv6-address	(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. **Note** The *IPv6-address* argument is not supported in Cisco IOS XE Denali 16.3.1.
vrf *vrf-name*	(Optional) Enables debugging operations for the virtual routing and forwarding instance.
detail	(Optional) Displays detailed logs of NHRP debugs.
error	(Optional) Enables NHRP error debugging operations.
extension	(Optional) Enables NHRP extension processing debugging operations.
group	(Optional) Enables NHRP group debugging operations.
packet	(Optional) Enables NHRP activity debugging.
rate	(Optional) Enables NHRP rate limiting.
routing	(Optional) Enables NHRP routing debugging operations.

Command Default

NHRP debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *IPv6-nbma-address* argument although available on the switch, will not work if configured.

Use the **debug nhrp detail** command to view the NHRP attribute logs.

The **Virtual-Access** *number* keyword-argument pair is visible only if the virtual access interface is available on the device.

Examples

The following sample output from the **debug nhrp** command displays NHRP debugging output for IPv4:

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

fhrp delay

To specify the delay period for the initialization of First Hop Redundancy Protocol (FHRP) clients, use the **fhrp delay** command in interface configuration mode. To remove the delay period specified, use the **no** form of this command.

fhrp delay {[**minimum**] [**reload**] *seconds*}
no fhrp delay {[**minimum**] [**reload**] *seconds*}

Syntax Description

minimum	(Optional) Configures the delay period after an interface becomes available.
reload	(Optional) Configures the delay period after the device reloads.
seconds	Delay period in seconds. The range is from 0 to 3600.

Command Default

None

Command Modes

Interface configuration (config-if)

Examples

This example shows how to specify the delay period for the initialization of FHRP clients:

```
Device(config-if)# fhrp delay minimum 90
```

Related Commands

Command	Description
show fhrp	Displays First Hop Redundancy Protocol (FHRP) information.

fhrp version vrrp v3

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) and Virtual Router Redundancy Service (VRRS) configuration on a device, use the **fhrp version vrrp v3** command in global configuration mode. To disable the ability to configure VRRPv3 and VRRS on a device, use the **no** form of this command.

fhrp version vrrp v3
no fhrp version vrrp v3

Syntax Description

This command has no keywords or arguments.

Command Default

VRRPv3 and VRRS configuration on a device is not enabled.

Command Modes

Global configuration (config)

Usage Guidelines

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable.

Examples

In the following example, a tracking process is configured to track the state of an IPv6 object using a VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20:

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

Related Commands

Command	Description
track (VRRP)	Enables an object to be tracked using a VRRPv3 group.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

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

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

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

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

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

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

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

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

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

Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

To transparently bridge IP on an interface, you must perform the following two tasks:

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

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

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp** command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the device. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Usage Guidelines

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the device.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type* is the Ethernet interface where the command is configured and *interface-type number* is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number* option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

If a Cisco device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the device. However, you can use the **ip address dhcp hostname**

hostname command to place a different name in the DHCP option 12 field than the globally configured hostname of the device.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 1: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the device in the option 12 field.
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the device in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a device configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

The DISCOVER message sent by a device configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
```

```
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a Dynamic Host Configuration Protocol (DHCP) pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

ip address pool *name*
no ip address pool

Syntax Description

name	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in *name*.

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

Usage Guidelines

Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the device. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.

Examples

The following example specifies that the IP address of GigabitEthernet interface 1/0/1 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip nhrp authentication

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

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

Syntax Description

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 (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

All devices 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:

```
Device(config-if)# ip nhrp authentication specialxx
```

ip nhrp holdtime

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

ip nhrp holdtime *seconds*
no ip nhrp holdtime [*seconds*]

Syntax Description

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 (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

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

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

Examples

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
Device(config-if)# ip nhrp holdtime 3600
```

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-ip-address*][*dest-mask*][*nbma-ipv6-address*] | **multicast** {*nbma-ip-address nbma-ipv6-address* | **dynamic**}}
no ip nhrp map {*ip-address* [*nbma-ip-address*][*dest-mask*][*nbma-ipv6-address*] | **multicast** {*nbma-ip-address nbma-ipv6-address* | **dynamic**}}

Syntax Description

ip-address	IP address of the destinations reachable through the Nonbroadcast multiaccess (NBMA) network. This address is mapped to the NBMA address.
nbma-ip-address	NBMA IP address.
dest-mask	Destination network address for which a mask is required.
nbma-ipv6-address	NBMA IPv6 address.
dynamic	Dynamically learns destinations from client registrations on hub.
multicast	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.

Command Default

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

You will probably need to configure at least one static mapping in order to reach the next-hop server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 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.

```
Device(config)# interface tunnel 0
Device(config-if)# ip nhrp nhs 10.0.0.1
Device(config-if)# ip nhrp nhs 10.0.1.3
Device(config-if)# ip nhrp map 10.0.0.1 192.0.0.1
Device(config-if)# ip nhrp map 10.0.1.3 192.2.7.8
```

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.

```
Device(config)# interface tunnel 0
Device(config-if)# ip address 10.0.0.3 255.0.0.0
Device(config-if)# ip nhrp map multicast 10.0.0.1
Device(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

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

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 {*ip-nbma-address ipv6-nbma-address* | **dynamic**}
no ip nhrp map multicast {*ip-nbma-address ipv6-nbma-address* | **dynamic**}

Syntax Description

ip-nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium that you are using.
ipv6-nbma-address	IPv6 NBMA address. **Note** This argument is not supported in Cisco IOS XE Denali 16.3.1.
dynamic	Dynamically learns destinations from client registrations on the hub.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

This command applies only to tunnel interfaces. This 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:

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

Command	Description
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
tunnel destination	Specifies the destination for a tunnel interface.

ip nhrp network-id

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

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

Syntax Description

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 (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

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

Examples

The following example enables NHRP on the interface:

```
Device(config-if)# ip nhrp network-id 1
```

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs**command in interface configuration mode. To remove the address, use the **no** form of this command.

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-addressFQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-addressFQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*]}
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*]}

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.

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
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

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:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(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:

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

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

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(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 registration

To set the time between periodic registration messages in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp registration** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ip nhrp registration timeout *seconds*
no ip nhrp registration timeout *seconds*

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.

Command Default

This command is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

Use this command to set the time between periodic registration in the Next Hop Resolution Protocol (NHRP) request and reply packets.

Examples

The following example shows that the registration timeout is set to 120 seconds:

```
Device(config)# interface tunnel 4
Device(config-if)# ip nhrp registration timeout 120
```

Related Commands

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

ipv6 nd cache expire

To configure the duration of time before an IPv6 neighbor discovery cache entry expires, use the **ipv6 nd cache expire** command in the interface configuration mode. To remove this configuration, use the **no** form of this command.

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

Syntax Description

expire-time-in-seconds	The time range is from 1 through 65536 seconds. The default is 14 or 4 hours.
refresh	(Optional) Automatically refreshes the neighbor discovery cache e

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced for the Cisco Catalyst 9500 Se

Usage Guidelines

By default, a neighbor discovery cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds or 4 hours. The **ipv6 nd cache expire** command allows the expiry time to vary and to trigger auto refresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, a neighbor discovery cache entry is auto refreshed. The entry moves into the DELAY state and the neighbor unreachability detection process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation is sent and then retransmitted as per the configuration.

Examples

The following example shows that the neighbor discovery cache entry is configured to expire in 7200 seconds or 2 hours:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

Related Commands

Command	Description
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd na glean

To configure the neighbor discovery to glean an entry from an unsolicited neighbor advertisement, use the **ipv6 nd na glean** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced for the Cisco Catalyst 950

Usage Guidelines

IPv6 nodes may emit a multicast unsolicited neighbor advertisement packet following the successful completion of duplicate address detection (DAD). By default, other IPv6 nodes ignore these unsolicited neighbor advertisement packets. The **ipv6 nd na glean** command configures the router to create a neighbor advertisement entry on receipt of an unsolicited neighbor advertisement packet (assuming no such entry already exists and the neighbor advertisement has the link-layer address option). Use of this command allows a device to populate its neighbor advertisement cache with an entry for a neighbor before data traffic exchange with the neighbor.

Examples

The following example shows how to configure neighbor discovery to glean an entry from an unsolicited neighbor advertisement:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery cache entry expires.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd nud retry

To configure the number of times the neighbor unreachability detection process resends neighbor solicitations, use the **ipv6 nd nud retry** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}
no ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}

Syntax Description

base	The neighbor unreachability detection process base value.
interval	The time interval, in milliseconds, between retries. The range is from 1000 to 32000.
max-attempts	The maximum number of retry attempts, depending on the base val The range is from 1 to 128.
final-wait-time	The waiting time, in milliseconds, on the last probe. The range is from 1000 to 32000.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced for the Cisco Catalyst 9500 Se

Usage Guidelines

When a device runs neighbor unreachability detection to resolve the neighbor detection entry for a neighbor again, it sends three neighbor solicitation packets 1 second apart. In certain situations, for example, spanning-tree events, or high-traffic events, or end-host reloads), three neighbor solicitation packets that are sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for neighbor solicitation retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm^n

here,

- t = Time interval
- m = Base (1, 2, or 3)
- n = Current neighbor solicitation number (where the first neighbor solicitation is 0).

Therefore, **ipv6 nd nud retry 3 1000 5** command retransmits at intervals of 1,3,9,27,81 seconds. If the final wait time is not configured, the entry remains for 243 seconds before it is deleted.

The **ipv6 nd nud retry** command affects only the retransmit rate for the neighbor unreachability detection process, and not for the initial resolution, which uses the default of three neighbor solicitation packets sent 1 second apart.

Examples

The following example shows how to configure a fixed interval of 1 second and three retransmits:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example shows how to configure a retransmit interval of 1, 2, 4, and 8:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example shows how to configure the retransmit intervals of 1, 3, 9, 27, 81:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain *name-of-chain*
no key chain *name-of-chain*

Syntax Description

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.

Command Default

No key chain exists.

Command Modes

Global configuration (config)

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example shows how to specify key chain:

```
Device(config-keychain-key)# key-string chestnut
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string **key-string** *text*
no **key-string** *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Examples

The following example shows how to specify the authentication string for a key:

```
Device(config-keychain-key)# key-string key1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

key-id	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

Command Default

No key exists on the key chain.

Command Modes

Command Modes Key-chain configuration (config-keychain)

Usage Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example shows how to specify a key to identify authentication on a key-chain:

```
Device(config-keychain)#key 1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

show ip nat translations

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

show ip nat translations [**inside** *global-ip*] [**outside** *local-ip*] [**icmp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name*]

Syntax Description

icmp	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
inside *global-ip*	(Optional) Displays entries for only a specific inside global IP address.
outside *local-ip*	(Optional) Displays entries for only a specific outside local IP address.
tcp	(Optional) Displays TCP protocol entries.
udp	(Optional) Displays User Datagram Protocol (UDP) entries.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes

EXEC

Command History

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

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

```
Router# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.69.233.209     192.168.1.95       ---                ---
--- 10.69.233.210     192.168.1.89       ---                --
```

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

```
Router# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
```

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

```
Router# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
udp 172.16.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
        create 00:00:02, use 00:00:00, flags: extended
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 172.16.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
        create 00:00:02, use 00:00:00, flags: extended
```

The following is sample output that includes the **vrf** keyword:

```
Router# show ip nat translations vrf
abc
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.1            192.168.121.113    ---                ---
--- 10.2.2.2            192.168.122.49     ---                ---
--- 10.2.2.11           192.168.11.1       ---                ---
--- 10.2.2.12           192.168.11.3       ---                ---
--- 10.2.2.13           172.16.5.20        ---                ---
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.3            192.168.121.113    ---                ---
--- 10.2.2.4            192.168.22.49      ---                ---
```

The following is sample output that includes the **inside**keyword:

```
Router# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is sample output when NAT that includes the **inside**keyword:

```
Router# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is a sample output that displays information about NAT port parity and conservation:

```
Router# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  200.200.0.100:5066    100.100.0.56:5066     200.200.0.56:5060     200.200.0.56:5060
udp  200.200.0.100:1025    100.100.0.57:10001    200.200.0.57:10001    200.200.0.57:10001
udp  200.200.0.100:10000   100.100.0.56:10000    200.200.0.56:10000    200.200.0.56:10000
udp  200.200.0.100:1024    100.100.0.57:10000    200.200.0.57:10000    200.200.0.57:10000
udp  200.200.0.100:10001   100.100.0.56:10001    200.200.0.56:10001    200.200.0.56:10001
udp  200.200.0.100:9985    100.100.0.57:5066     200.200.0.57:5060     200.200.0.57:5060
Total number of translations: 6
```

The table below describes the significant fields shown in the display.

Table 2: show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.

Field	Description
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended--Extended translation • static--Static translation • destination--Rotary translation • outside--Outside translation • timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

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.
show ip nat statistics	Displays NAT statistics.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs**command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [{*interface*}] [**detail**] [{**redundancy** [{**cluster** *number* | **preempted** | **running** | **waiting**}]}]

Syntax Description

interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays information about NHS redundancy stacks.
cluster *number*	(Optional) Displays redundancy cluster information.
preempted	(Optional) Displays information about NHS that failed to become active and is preempted.
running	(Optional) Displays NHSs that are currently in Responding or Expecting replies states.
waiting	(Optional) Displays NHSs awaiting to be scheduled.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 3: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
ANI	0 to 1000	Autonomic-Networking virtual interface
Auto-Template	1 to 999	Auto-Template interface
GMPLS	0 to 1000	Multiprotocol Label Switching (MPLS) interface
GigabitEthernet	0 to 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 to 9	Internal interface

Valid Types	Number Ranges	Interface Descriptions
LISP	0 to 65520	Locator/ID Separation Protocol (LISP) virtual interface
loopback	0 to 2147483647	Loopback interface
Null	0 to 0	Null interface
PROTECTION_GROUP	0 to 0	Protection-group controller
Port-channel	1 to 128	Port channel interface
TenGigabitEthernet	0 to 9	TenGigabitEthernet interface
Tunnel	0 to 2147483647	Tunnel interface
Tunnel-tp	0 to 65535	MPLS Transport Profile interface
Vlan	1 to 4094	VLAN interface

Examples

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

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
   10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

The table below describes the significant field shown in the display.

Table 4: show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.

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.

show ip ports all

To display all the open ports on a device, use the **show ip ports all** in user EXEC or privileged EXEC mode.

show ip ports all

Syntax Description

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

To close open ports, you can use one of the following methods:

- Use Access Control List (ACL).
- To close the UDP 2228 port, use the **no l2 traceroute** command.
- To close TCP 80, TCP 443, TCP 6970, TCP 8090 ports, use the **no ip http server** and **no ip http secure-server** commands.

Examples

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

```
Device#
show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *:* LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
udp *:10002 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

The table below describes the significant fields shown in the display

Table 5: Field Descriptions of show ip ports all

Field	Description
Protocol	Transport protocol used.

Field	Description
Local Address.	Device IP Address.
Foreign Address	Remote or peer address.
State	State of the connection. It can be listen, established or connected.
PID/Program Name	Process ID or name

Related Commands

Command	Description
show tcp brief all	Displays information about TCP connection endpoints.
show ip sockets	Displays IP sockets information.

show key chain

To display the keychain, use the **show key chain** command.

show key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the key chain command.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

Privileged EXEC (#)

Examples

The following is sample output from the **show key chain** command:

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

Related Commands

Command	Description
key-string	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [{*object-number* **[brief]** | **application** **[brief]** | **interface** **[brief]** | **ip[route [brief]** | **[sla [brief]]** | **ipv6** **[route [brief]]** | **list** **[route [brief]]** | **resolution** **[ip** | **ipv6]** | **stub-object** **[brief]** | **summary** | **timers**}]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
application	(Optional) Displays tracked application objects.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP route objects.
ip sla	(Optional) Displays tracked IP SLA objects.
ipv6 route	(Optional) Displays tracked IPv6 route objects.
list	(Optional) Displays the list of boolean objects.
resolution	(Optional) Displays resolution of tracked parameters.
summary	(Optional) Displays the summary of the specified object.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Device# show track 1

Track 1
 Interface GigabitEthernet 1/0/1 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

The table below describes the significant fields shown in the displays.

Table 6: show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface GigabitEthernet 1/0/1 ip routing	Interface type, interface number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.

Related Commands

Command	Description
show track resolution	Displays the resolution of tracked parameters.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

track

To configure an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface, use the **track** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}
no track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}

Syntax Description

object-number	Object number in the range from 1 to 1000 representing the interface to be tracked.
interface *type number*	Interface type and number to be tracked.
line-protocol	Tracks whether the interface is up.
ip routing	Tracks whether IP routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.
ipv6 routing	Tracks whether IPv6 routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.

Command Default

The state of the interfaces is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced..

Usage Guidelines

Use the **track** command in conjunction with the **glbp weighting** and **glbp weighting track** commands to configure parameters for an interface to be tracked. If a tracked interface on a GLBP device goes down, the weighting for that device is reduced. If the weighting falls below a specified minimum, the device will lose its ability to act as an active GLBP virtual forwarder.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, TenGigabitEthernet interface 0/0/1 tracks whether GigabitEthernet interfaces 1/0/1 and 1/0/3 are up. If either of the GigabitEthernet interface goes down, the GLBP weighting is reduced by the default value of 10. If both GigabitEthernet interfaces go down, the GLBP weighting will fall below the lower threshold and the device will no longer be an active forwarder. To resume its role as an active forwarder, the device must have both tracked interfaces back up, and the weighting must rise above the upper threshold.

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

vrrp

To create a Virtual Router Redundancy Protocol version 3 (VRRPv3) group and enter VRRPv3 group configuration mode, use the **vrrp**. To remove the VRRPv3 group, use the **no** form of this command.

vrrp *group-id* **address-family** {**ipv4** | **ipv6**}
no **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}

Syntax Description

group-id	Virtual router group number. The range is from 1 to 255.
address-family	Specifies the address-family for this VRRP group.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced..

Usage Guidelines

Examples

The following example shows how to create a VRRPv3 group and enter VRRP configuration mode:

```
Device(config-if)# vrrp 3 address-family ipv4
```

Related Commands

Command	Description
timers advertise	Sets the advertisement timer in milliseconds.

vrrp description

To assign a description to the Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *text*
no description

Syntax Description

text	Text (up to 80 characters) that describes the purpose or use of the group.

Command Default

There is no description of the VRRP group.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

The following example enables VRRP. VRRP group 1 is described as Building A – Marketing and Administration.

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

vrrp preempt

To configure the device to take over as master virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current master virtual router, use the **preempt** command in VRRP configuration mode. To disable this function, use the **no** form of this command.

preempt [**delay** **minimum** *seconds*]
no **preempt**

Syntax Description

delay minimum *seconds*	(Optional) Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.

Command Default

This command is enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

By default, the device being configured with this command will take over as master virtual router for the group if it has a higher priority than the current master virtual router. You can configure a delay, which will cause the VRRP device to wait the specified number of seconds before issuing an advertisement claiming master ownership.

Note The device that is the IP address owner will preempt, regardless of the setting of this command.

Examples

The following example configures the device to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router. If the device preempts the current master virtual router, it waits 15 seconds before issuing an advertisement claiming it is the master virtual router.

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
priority	Sets the priority level of the device within a VRRP group.

vrrp priority

To set the priority level of the device within a Virtual Router Redundancy Protocol (VRRP) group, use the **priority** command in interface configuration mode. To remove the priority level of the device, use the **no** form of this command.

priority *level*
no priority *level*

Syntax Description

level	Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.

Command Default

The priority level is set to the default value of 100.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Use this command to control which device becomes the master virtual router.

Examples

The following example configures the device with a priority of 254:

```
Device(config-if-vrrp)# priority 254
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
vrrp preempt	Configures the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual router.

vrrp timers advertise

To configure the interval between successive advertisements by the master virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the **timers advertise** command in VRRP configuration mode. To restore the default value, use the **no** form of this command.

timers advertise [**msec**] *interval*
no timers advertise [**msec**] *interval*

Syntax Description

group	Virtual router group number. The group number range is from 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.
interval	Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the **msec** keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the **msec** keyword is specified, the valid range is 50 to 999 milliseconds.

Command Default

The default interval of 1 second is configured.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer values are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer values. If the same timer values are not set, the devices in the VRRP group will not communicate with each other and any misconfigured device will change its state to master.

Examples

The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

Command	Description
timers learn	Configures the device, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the master virtual router.

vrrs leader

To specify a leader’s name to be registered with Virtual Router Redundancy Service (VRRS), use the **vrrs leader** command. To remove the specified VRRS leader, use the **no** form of this command.

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description

vrrs-leader-name	Name of VRRS Tag to lead.

Command Default

A registered VRRS name is unavailable by default.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Examples

The following example specifies a leader's name to be registered with VRRS:

```
Device(config-if-vrrp)# vrrs leader leader-1
```

Related Commands

Command	Description
vrrp	Creates a VRRP group and enters VRRP configuration mode.