



## NHRP Commands

---

# clear ip nhrp

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

```
clear ip nhrp [dest_ip-address [dest_mask]] | [counters {interface if-name if-number | vrf
vrf-name }] | [shortcut [interface if-name if-number ]]
```

Syntax Description		
<i>dest_ip-address</i>	(Optional) Clears NHRP mapping entries for specified destination IP addresses.	
<i>dest_mask</i>	(Optional) Name of the destination network mask.	
<b>counters</b>	(Optional) Clears the NHRP counters.	
<b>interface</b>	(Optional) Clears NHRP mapping entries for the specified interface.	
<i>if-name</i>	(Optional) Interface name. Specifying this arguments removes the specified interface name that all entries learned via this interface from the Next Hop Resolution Protocol (NHRP) cache.	
<i>if-number</i>	(Optional) Interface number. Specifying this arguments removes the specified interface number that all entries learned via this interface from the Next Hop Resolution Protocol (NHRP) cache.	
<b>vrf</b>	(Optional) Deletes entries from the Next Hop Resolution Protocol (NHRP) cache for the specified VRF.	
<i>vrf-name</i>	(Optional) Name of the VRF address-family to which the command is applied.	
<b>shortcut</b>	(Optional) Deletes shortcut entries from the Next Hop Resolution Protocol (NHRP) cache.	

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	11.0	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.
	Cisco IOS XE Release 2.5	This command was modified. Support was added for the <b>shortcut</b> keyword.

Usage Guidelines	
	This command does not clear any static (configured) IP-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache. The <b>clear ip nhrp shortcut</b> command clears NHRP cache entries that have associated NHRP routes/nexthop-overrides in the RIB.

---

**Examples**

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

```
Router> clear ip nhrp
```

The following example shows how to clear NHRP cache entries that have associated NHRP routes/next-hop overrides in the RIB:

```
Router> clear ip nhrp shortcut
```

---

**Related Commands**

Command	Description
show ip nhrp	Displays the NHRP cache.

# ip nhrp authentication

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

**ip nhrp authentication** *string*

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

## Syntax Description

<i>string</i>	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.
---------------	---

## Defaults

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

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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

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	
	<i>group-name</i> 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.

Usage Guidelines	
	After you create an NHRP group on a spoke, you use the <b>ip nhrp map group</b> 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
	<b>ip nhrp map group</b>	Adds NHRP groups to QoS policy mappings on a hub.
	<b>show dmvpn</b>	Displays DMVPN-specific session information.
	<b>show ip nhrp</b>	Displays NHRP mapping information.
	<b>show ip nhrp group-map</b>	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.
	<b>show policy-map mgre</b>	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 in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip nhrp holdtime** *seconds*

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

### Syntax Description

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

### Defaults

7200 seconds (2 hours)

### Command Modes

Interface configuration

### Command History

Release	Modification
10.3	This command was introduced.
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 in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip nhrp interest** *access-list-number*

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

## Syntax Description

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

## Defaults

All non-NHRP packets can trigger NHRP requests.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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
<b>access-list (IP extended)</b>	Defines an extended IP access list.

<b>Command</b>	<b>Description</b>
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>ip nhrp use</b>	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
```

```
no ip nhrp map ip-address nbma-address
```

## Syntax Description

<i>ip-address</i>	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
<i>nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.

## Defaults

No static IP-to-NBMA cache entries exist.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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

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
 ip nhrp map 10.0.1.3 192.2.7.8
```

Related Commands\	Command	Description
	<b>clear ip nhrp</b>	Clears all dynamic entries from the NHRP cache.

# 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

<i>group-name</i>	Specifies an NHRP group name.
<i>qos-policy-map-name</i>	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.

## 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
	<b>ip nhrp group</b>	Configures a NHRP group on a spoke.
	<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
	<b>show dmvpn</b>	Displays DMVPN-specific session information.
	<b>show ip nhrp</b>	Displays NHRP mapping information.
	<b>show ip nhrp group-map</b>	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.
	<b>show policy-map mgre</b>	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

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

## Defaults

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

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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

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.

**Defaults** 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 <b>no</b> form of this command.

## Usage Guidelines

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

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
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1436
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
```

```
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 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		
	<i>pkt-count</i>	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
	<b>every</b> <i>seconds</i>	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults	
	<i>pkt-count</i> : 100 packets
	<i>seconds</i> : 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 consideration 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
<b>ip nhrp interest</b>	Controls which IP packets can trigger sending an NHRP request.
<b>ip nhrp use</b>	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

# ip nhrp network-id

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

**ip nhrp network-id** *number*

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

## Syntax Description

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

## Defaults

NHRP is disabled on the interface.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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-address | FQDN-string}] [multicast] [priority value]
[cluster value] | cluster value max-connections value | dynamic nbma {nbma-address |
FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
```

```
no ip nhrp nhs {nhs-address [nbma {nbma-address | FQDN-string}] [multicast] [priority value]
[cluster value] | cluster value max-connections value | dynamic nbma {nbma-address |
FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
```

### Syntax Description

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

### Defaults

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 <i>net-address</i> and <i>mask</i> arguments were removed and the <b>nbma</b> , <i>nbma-address</i> , <i>FQDN-string</i> , <b>multicast</b> , <b>priority value</b> , <b>cluster value</b> , <b>max-connections value</b> , <b>dynamic</b> , and <b>fallback seconds</b> keywords and arguments were added.

**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.

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
	<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
	<b>show ip nhrp</b>	Displays NHRP mapping information.

# ip nhrp record

To reenble the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp record** interface configuration command. To suppress the use of such options, use the **no** form of this command.

**ip nhrp record**

**no ip nhrp record**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Forward record and reverse record options are used in NHRP request and reply packets.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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
<b>ip nhrp responder</b>	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*]

<b>Syntax Description</b>	<b>timeout</b> <i>seconds</i>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
<code>ip nhrp shortcut</code>	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**]

**no ip nhrp registration** [*timeout seconds* | **no-unique**]

Syntax Description	timeout <i>seconds</i>	(Optional) Time between periodic registration messages.
		<ul style="list-style-type: none"> <li><i>seconds</i>—Number of seconds. The range is from 1 through the value of the NHRP hold timer.</li> <li>If the <b>timeout</b> keyword is not specified, NHRP registration messages are sent every number of seconds equal to 1/3 the value of the NHRP hold timer.</li> </ul>
	<b>no-unique</b>	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.

**Defaults** This command is not enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.3	This command was introduced.
	12.3(7.2)	The <b>timeout</b> keyword and <i>seconds</i> argument were added. In addition, effective with Cisco IOS Release 12.3(7.2), this command replaced the <b>ip nhrp registration no-unique</b> command.
	12.3(7)T	The <b>timeout</b> keyword and <i>seconds</i> argument were integrated into Cisco IOS Release 12.3(7)T. In addition, the replacement of the <b>ip nhrp registration no-unique</b> 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.

**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.

---

**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
```

---

**Related Commands**

Command	Description
<b>ip nhrp holdtime</b>	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 in interface 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

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

## Defaults

The next-hop server uses the IP address of the interface where the NHRP request was received.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.3	This command was introduced.
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 server-only

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

**ip nhrp server-only [non-caching]**

**no ip nhrp server-only**

### Syntax Description

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

### Defaults

Disabled

### Command Modes

Interface configuration

### Command History

Release	Modification
11.2	This command was introduced.
12.0	The <b>non-caching</b> 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 disabled.

**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.

**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
	<b>ip nhrp redirect</b>	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 in interface configuration mode. To restore the default thresholds, use the **no** form of this command.

**ip nhrp trigger-svc** *trigger-threshold* *teardown-threshold*

**no ip nhrp trigger-svc**

### Syntax Description

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

### Defaults

*trigger-threshold*: 1 kbps  
*teardown-threshold*: 0 kbps

### Command Modes

Interface configuration

### Command History

Release	Modification
12.0	This command was introduced.
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**

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

# ip nhrp use

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

**ip nhrp use** *usage-count*

**no ip nhrp use** *usage-count*

## Syntax Description

*usage-count* Packet count in the range from 1 to 65535. Default is 1.

## Defaults

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

## Command Modes

Interface configuration

## Command History

Release	Modification
11.1	This command was introduced.
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
<b>ip nhrp interest</b>	Controls which IP packets can trigger sending an NHRP request.
<b>ip nhrp max-send</b>	Changes the maximum frequency at which NHRP packets can be sent.

# show ip nhrp

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

```
show ip nhrp [dynamic | incomplete | static] [address | interface] [brief | detail] [purge]
[shortcut]
```

Syntax Description		
<b>dynamic</b>	(Optional)	Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See <a href="#">Table 40</a> for types, number ranges, and descriptions.
<b>incomplete</b>	(Optional)	Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See <a href="#">Table 40</a> for types, number ranges, and descriptions.
<b>static</b>	(Optional)	Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the <b>ip nhrp map</b> command. See <a href="#">Table 40</a> for types, number ranges, and descriptions.
<i>address</i>	(Optional)	Displays NHRP mapping entries for specified protocol addresses.
<i>interface</i>	(Optional)	Displays NHRP mapping entries for the specified interface. See <a href="#">Table 40</a> for types, number ranges, and descriptions.
<b>brief</b>	(Optional)	Displays a short output of the NHRP mapping.
<b>detail</b>	(Optional)	Displays detailed information about NHRP mapping.
<b>purge</b>	(Optional)	Displays NHRP purge information.
<b>shortcut</b>	(Optional)	Displays NHRP shortcut information.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command Default	
	Information is displayed for all NHRP mappings.

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.
	12.4(22)T	The output of this command was extended to display the NHRP group received from the spoke.
	Cisco IOS XE Release 2.5	This command was modified. Support was added for the <b>shortcut</b> keyword.

**Usage Guidelines**

Table 40 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 40** Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
<b>async</b>	1	Async
<b>atm</b>	0 to 6	ATM
<b>bvi</b>	1 to 255	Bridge-Group Virtual Interface
<b>cdma-ix</b>	1	CDMA Ix
<b>ctunnel</b>	0 to 2147483647	C-Tunnel
<b>dialer</b>	0 to 20049	Dialer
<b>ethernet</b>	0 to 4294967295	Ethernet
<b>fastethernet</b>	0 to 6	FastEthernet IEEE 802.3
<b>lex</b>	0 to 2147483647	Lex
<b>loopback</b>	0 to 2147483647	Loopback
<b>mfr</b>	0 to 2147483647	Multilink Frame Relay bundle
<b>multilink</b>	0 to 2147483647	Multilink-group
<b>null</b>	0	Null
<b>port-channel</b>	1 to 64	Port channel
<b>tunnel</b>	0 to 2147483647	Tunnel
<b>vif</b>	1	PGM multicast host
<b>virtual-ppp</b>	0 to 2147483647	Virtual PPP
<b>virtual-template</b>	1 to 1000	Virtual template
<b>virtual-tokenring</b>	0 to 2147483647	Virtual Token Ring
<b>xtagatm</b>	0 to 2147483647	Extended tag ATM

**Examples**

The following is sample output from the **show ip nhrp** command. This output shows the NHRP group received from the spoke:

```
Router# show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:17:49, expire 00:01:30
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-0
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:11, expire 01:59:48
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.3
  Group: test-group-0
11.0.0.2/32 via 11.0.0.2, Tunnel1 created 00:17:49, expire 00:02:10
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
```

```
Group: test-group-1
```

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

```
Router#show ip nhrp shortcut

10.1.1.1/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
  Type: dynamic, Flags: router rib
  NBMA address: 10.12.1.1
10.1.1.2/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
  Type: dynamic, Flags: router rib nho
  NBMA address: 10.12.1.2
```

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

```
Router# show ip nhrp detail

10.1.1.1/8 via 10.2.1.1, Tunnel1 created 00:46:29, never expire
  Type: static, Flags: used
  NBMA address: 10.12.1.1
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
  Type: dynamic, Flags: authoritative unique nat registered used
  NBMA address: 10.12.1.2
10.1.1.4, Tunnel1 created 00:00:07, expire 00:02:57
  Type: incomplete, Flags: negative
  Cache hits: 4
```

Table 41 describes the significant fields shown in the displays.

**Table 41** show ip nhrp Field Descriptions

Field	Description
10.1.1.1/8	Target network.
via 10.2.1.1	Next Hop to reach the target network.
Tunnel1	Interface through which the target network is reached.
created 00:00:12	Length of time since the entry was created (hours:minutes:seconds).
expire 01:59:47	Time remaining until the entry expires (hours:minutes:seconds).
never expire	Indicates that static entries never expire.
Type	<ul style="list-style-type: none"> <li>dynamic—NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations.</li> <li>static—NHRP mapping is configured statically. Entries configured by the <b>ip nhrp map</b> command are marked static.</li> <li>incomplete—The NBMA address is not known for the target network.</li> </ul>
NBMA address	Nonbroadcast multiaccess address of the next hop. The address format is appropriate for the type of network being used: ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel.

Table 41 *show ip nhrp Field Descriptions (continued)*

Field	Description
Flags	<ul style="list-style-type: none"> <li data-bbox="820 317 1502 436">• authoritative—Indicates that the NHRP information was obtained directly from the Next Hop Server or router that maintains and is authoritative for the NBMA-to-IP address mapping for a particular destination.</li> <li data-bbox="820 457 1502 611">• implicit—Indicates that the local node learned about the NHRP mapping entries from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router.</li> <li data-bbox="820 632 1502 1129">• local—Indicates NHRP mapping entries that are for networks local to this router (that is, serviced by this router). These flag entries are created when this router answers an NHRP resolution request that has this information and is used to store the transport (tunnel) IP address of all the other NHRP nodes to which it has sent this information. If for some reason this router loses access to this local network (that is, it can no longer service this network), it sends an NHRP purge message to all remote NHRP nodes that are listed in the “local” entry (in <b>show ip nhrp detail</b> command output) to tell the remote nodes to clear this information from their NHRP mapping tables. This local mapping entry times out of the local NHRP mapping database at the same time that this information (from the NHRP resolution reply) would time out of the NHRP mapping database on the remote NHRP nodes.</li> <li data-bbox="820 1150 1502 1297">• nat—Indicates that the remote node (NHS client) supports the new NHRP NAT extension type for dynamic spoke-spoke tunnels to/from spokes behind a NAT router. This marking does not indicate that the spoke (NHS client) is behind a NAT router.</li> </ul>


Table 41 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	<ul style="list-style-type: none"> <li data-bbox="781 317 1463 632"> <p>• <b>negative</b>—For negative caching, indicates that the requested NBMA mapping has not yet been or could not be obtained.</p> <p>When NHRP sends an NHRP resolution request, an incomplete (negative) NHRP mapping entry for the address is inserted in the resolution request. This insertion suppresses any more triggering of NHRP resolution requests while the resolution request is being resolved. If configured, any encryption parameters (IKE/IPsec) for the tunnel are negotiated.</p> </li> <li data-bbox="781 646 1463 1556"> <p>• <b>(no socket)</b>—Indicates that the NHRP mapping entries will not trigger IPsec to set up encryption because data traffic does not need to use this tunnel. Later, if data traffic needs to use this tunnel, the flag will change from a “(no socket)” to a “(socket)” entry and IPsec will be triggered to set up the encryption for this tunnel. Local and implicit NHRP mapping entries are always initially marked as “(no socket).”</p> <p>By default, NHRP caches source information from NHRP resolution request or replies as they go through the system. To allow this caching to continue, but not have the entry create an IPsec socket, they are marked as (no socket). If this was not done there would be extra IPsec sockets from the hubs to the various spokes that either were not used or were used for only one or two packets while a direct spoke-to-spoke tunnel was being built. Data packets and NHRP packets that arrive on the tunnel interface and are forwarded back out the tunnel interface are not allowed to use the (no socket) NHRP mappings for forwarding. Because, in this case, the router is an intermediate node in the path between the two endpoints and we only want to create short-cut tunnels between the initial entrance and final exit point of the DMVPN (NBMA) network and not between any intermediate nodes. If at some point the router receives a data packet that has a source interface that is not the tunnel interface and it would use the (no socket) mapping entry, the router converts the (no socket) entry to a (socket) entry. In this case, this router is the entrance (or exit) point of the NBMA (for this traffic stream).</p> </li> </ul>

Table 41 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	<ul style="list-style-type: none"> <li data-bbox="818 317 1507 596">• (no socket) (continued)—These (no socket) mapping entries are marked (non-authoritative); only mappings from NHRP registrations are marked (authoritative). The NHRP resolution requests are also marked (authoritative), which means that the NHRP resolution request can be answered only from an (authoritative) NHRP mapping entry. A (no socket) mapping entry will not be used to answer an NHRP resolution request and the NHRP resolution request will be forwarded to the NHS of the nodes .</li> <li data-bbox="818 617 1507 896">• registered—Indicates that the mapping entry was created in response to an NHRP registration request. Although registered mapping entries are dynamic entries, they may not be refreshed through the “used” mechanism. Instead, these entries are refreshed by another NHRP registration request with the same transport (tunnel) IP to NBMA address mapping. The Next Hop Client (NHC) periodically sends NHRP registration requests to keep these mappings from expiring.</li> <li data-bbox="818 917 1507 1003">• router—Indicates that NHRP mapping entries for a remote router (that is accessing a network or host behind the remote router) are marked with the router flag.</li> <li data-bbox="818 1024 1507 1583">• unique—NHRP registration requests have the unique flag set on by default. This flag indicates that an NHRP mapping entry cannot be overwritten by a mapping entry that has the same IP address and a different NBMA address. When a spoke has a statically configured outside IP (NBMA) address, this is used to keep another spoke that is mis-configured with the same transport (tunnel) IP address from overwriting this entry. If a spoke has a dynamic outside IP (NBMA) address, you can configure the <b>ip nhrp registration no-unique</b> command on the spoke to clear this flag. This configuration allows the registered NHRP mapping entry for that spoke on the hub to be overwritten with a new NBMA address. This is necessary in this case because the spoke's outside IP (NBMA) address can change at any time. If the “unique” flag was set, the spoke would have to wait for the mapping entry on the hub to time out before it could register its new (NBMA) mapping.</li> </ul>

**Table 41** show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	<ul style="list-style-type: none"> <li>used—When data packets are process-switched and this mapping entry was used, the mapping entry is marked as used. The mapping database is checked every 60 seconds. If the used flag is set and more than 120 seconds remain until expire time, the used flag is cleared. If fewer than 120 seconds are left, this mapping entry is “refreshed” by the transmission of another NHRP resolution request.</li> </ul> <p> <b>Note</b> When using DMVPN Phase 3 in 12.4(6)T, CEF switched packets will also set the “used” flag, and these entries will be timed out and refreshed as described in the “used” flag description above.</p>

**Related Commands**

Command	Description
<b>ip nhrp group</b>	Configures a NHRP group on a spoke.
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>ip nhrp map group</b>	Adds NHRP groups to QoS policy mappings on a hub.
<b>ip nhrp shortcut</b>	Enables shortcut switching on the tunnel interface.
<b>show dmvpn</b>	Displays DMVPN-specific session information.
<b>show ip nhrp group-map</b>	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.
<b>show ip nhrp multicast</b>	Displays NHRP multicast mapping information.
<b>show ip nhrp nhs</b>	Displays NHRP Next Hop Server information.
<b>show ip nhrp summary</b>	Displays NHRP mapping summary information.
<b>show ip nhrp traffic</b>	Displays NHRP traffic statistics.
<b>show policy-map mgre</b>	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

# show ip nhrp group-map

To display the details of NHRP group mappings, use the **show ip nhrp group-map** command in user EXEC or privileged EXEC mode.

```
show ip nhrp group-map [group-name]
```

<b>Syntax Description</b>	<i>group-name</i>	(Optional) Name of an NHRP group mapping for which information will be displayed.
---------------------------	-------------------	---

**Command Default** Information is displayed for all NHRP group mappings.

**Command Modes** User EXEC (>)  
Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(22)T	This command was introduced.

**Usage Guidelines** This command displays the details on NHRP group mappings on the hub along with the list of tunnels using each of the NHRP groups defined in the mappings. In combination with the **show ip nhrp** command, this command lets you easily determine which QoS policy map is applied to a specific tunnel endpoint.

This command displays the details of the specified NHRP group mapping. The details include the associated QoS policy name and the list of tunnel endpoints using the QoS policy. If no option is specified, it displays the details of all NHRP group mappings.

**Examples** The following is sample output from the **show ip nhrp group-map** command:

```
Router# show ip nhrp group-map
Interface: Tunnel0
NHRP group: test-group-0
QoS policy: queueing
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
10.0.0.2/172.17.0.2
10.0.0.3/172.17.0.3

Interface: Tunnel1
NHRP group: test-group-1
QoS policy: queueing
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
11.0.0.2/172.17.0.2

NHRP group: test-group-2
QoS policy: p1
```

Tunnels using the QoS policy: None

The following is sample output from the **show ip nhrp group-map** command for an NHRP group named test-group-0:

```
Router# show ip nhrp group-map test-group-0
Interface: Tunnel0
NHRP group: test-group-0
QoS policy: queueing
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
10.0.0.2/172.17.0.2
10.0.0.3/172.17.0.3
```

Table 42 describes the significant fields shown in the displays.

**Table 42** *show ip nhrp group-map Field Descriptions*

Field	Description
Interface	Interface on which the policy is configured.
NHRP group	NHRP group associated with the QoS policy on the interface.
QoS policy	QoS policy configured on the interface.
Tunnels using the QoS Policy	List of tunnel endpoints using the QoS policy.
Tunnel destination overlay/transport address	Tunnel destination overlay address (such as the tunnel endpoint address).

#### Related Commands

Command	Description
<b>ip nhrp group</b>	Configures a NHRP group on a spoke.
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>ip nhrp map group</b>	Adds NHRP groups to QoS policy mappings on a hub.
<b>show dmvpn</b>	Displays DMVPN-specific session information.
<b>show ip nhrp</b>	Displays NHRP mapping information.
<b>show policy-map mgre</b>	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

# show ip nhrp multicast

To display Next Hop Resolution Protocol (NHRP) multicast mapping information, use the **show ip nhrp multicast** command in user EXEC or privileged EXEC mode.

```
show ip nhrp multicast [nbma-address | interface]
```

Syntax Description	
<i>nbma-address</i>	(Optional) Displays multicast mapping information for the specified NBMA address.
<i>interface</i>	(Optional) Displays all multicast mapping entries of the NHRP network for the interface. See <a href="#">Table 43</a> for types, number ranges, and descriptions.

Command Modes
User EXEC Privileged EXEC

Command History	Release	Modification
	12.4(7)	This command was introduced.

**Usage Guidelines** [Table 43](#) 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 43** Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null

**Table 43** Valid Types, Number Ranges, and Interface Descriptions (continued)

Valid Types	Number Ranges	Interface Descriptions
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

**Examples**

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

```
Router# show ip nhrp multicast

  I/F      NBMA address
Tunnel1   1.1.1.1      Flags: static
```

Table 44 describes the fields shown in the display.

**Table 44** show ip nhrp Field Descriptions

Field	Description
I/F	Interface associated with the multicast mapping entry.
NBMA address	Nonbroadcast Multiaccess Address to which multicast packets will be sent. The address format is appropriate for the type of network used: ATM, Ethernet, SMDS, or multipoint tunnel.
Flags	<ul style="list-style-type: none"> <li>static—Indicates that the multicast mapping entry is configured statically by the <b>ip nhrp map multicast</b> command.</li> <li>dynamic—Indicates that the multicast mapping entry is obtained dynamically. A multicast mapping entry is created for each registered Next Hop Client (NHC) when the <b>ip nhrp map multicast dynamic</b> command is configured.</li> </ul>

**Related Commands**

Command	Description
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>show ip nhrp</b>	Displays NHRP mapping information.
<b>show ip nhrp nhs</b>	Displays NHRP Next Hop Server information.
<b>show ip nhrp summary</b>	Displays NHRP mapping summary information.
<b>show ip nhrp traffic</b>	Displays NHRP traffic 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-type interface-number] [detail | redundancy [cluster number |
preempted | running | waiting]
```

## Syntax Description

<i>interface-type</i>	(Optional) Type of interface for which NHS information should be displayed. See <a href="#">Table 43</a> for types, number ranges, and descriptions.
<i>interface-number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
<b>detail</b>	(Optional) Displays detailed NHS information.
<b>redundancy</b>	(Optional) Displays NHS recovery information.
<b>cluster number</b>	(Optional) Displays NHS recovery information based on the cluster value. The range is from 0 to 10.
<b>preempted</b>	(Optional) Displays NHSs that are declared as down and not actively probed.
<b>running</b>	(Optional) Displays NHSs that are responding or expecting replies.
<b>waiting</b>	(Optional) Displays NHSs that are waiting to be scheduled.

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 <b>redundancy</b> , <b>cluster number</b> , <b>preempted</b> , <b>running</b> , and <b>waiting</b> keywords and argument were added.

## Usage Guidelines

[Table 43](#) lists the valid types, number ranges, and descriptions for the optional *interface-number* argument.



### Note

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

**Table 45 Valid Types, Number Ranges, and Interface Descriptions**

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	Fast Ethernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

**Examples**

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

```
Router# 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 following is sample output from the **show ip nhrp nhs** command:

```
Router# show ip nhrp nhs
```

Legend: E=Expecting replies, R=Responding, W=Waiting

Tunnel0:

```
192.0.2.1 W priority = 2 cluster = 0
```

```
192.0.2.2 RE priority = 0 cluster = 0
```

```
192.0.2.3 RE priority = 1 cluster = 0
```

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

```
Router# show ip nhrp nhs redundancy
```

Legend: E=Expecting replies, R=Responding, W=Waiting

```
No.  Interface  Cluster  NHS           Priority  Cur-State  Cur-Queue  Prev-State  Prev-Queue
1    Tunnel0    0        10.0.0.253   3         RE         Running    E           Running
2    Tunnel0    0        10.0.0.252   2         RE         Running    E           Running
3    Tunnel0    0        10.0.0.251   1         RE         Running    E           Running
```

```
No.  Interface  Cluster  Status  Max-Con  Total-NHS  Responding  Expecting  Waiting  Fallback
1    Tunnel0    0        Enable  3        3          3           0          0        0
```

Table 44 describes the significant fields shown in the displays.

**Table 46** *show ip nhrp nhs Field Descriptions*

Field	Description
Tunnel1	Interface through which the target network is reached.
priority	Priority value assigned to the NHS.
cluster	Group to which the NHS belong to.
W=Waiting	NHSs that are preempted and are not in the active probe list.
E=Expecting replies	NHSs that are active and expecting replies.
R=Responding	NHSs that are active and responding.

#### Related Commands

Command	Description
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>show ip nhrp</b>	Displays NHRP mapping information.
<b>show ip nhrp multicast</b>	Displays NHRP multicast mapping information.
<b>show ip nhrp summary</b>	Displays NHRP mapping summary information.
<b>show ip nhrp traffic</b>	Displays NHRP traffic statistics.

# show ip nhrp summary

To display Next Hop Resolution Protocol (NHRP) mapping summary information, use the **show ip nhrp summary** command in user EXEC or privileged EXEC mode.

**show ip nhrp summary**

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS release 12.2(33)SRB.
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 is sample output from the **show ip nhrp summary** command:

```
Router# show ip nhrp summary

IP NHRP cache 1 entry, 256 bytes
  1 static 0 dynamic 0 incomplete
```

[Table 47](#) describes the significant field shown in the display.

**Table 47** *show ip nhrp summary Field Descriptions*

Field Output	Description
dynamic	NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations
static	NHRP mapping is configured statically. Entries configured by the <b>ip nhrp map</b> command are marked static.
incomplete	NBMA address is not known for the target network.

## Related Commands

Command	Description
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>show ip nhrp</b>	Displays NHRP mapping information.
<b>show ip nhrp multicast</b>	Displays NHRP multicast mapping information.
<b>show ip nhrp nhs</b>	Displays NHRP Next Hop Server information.
<b>show ip nhrp traffic</b>	Displays NHRP traffic statistics.

# show ip nhrp traffic

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

**show ip nhrp traffic** [**interface tunnel** *number*]

Syntax Description	interface	(Optional) Displays NHRP traffic information for a given interface.
	tunnel <i>number</i>	(Optional) Specifies the tunnel interface number.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.4(6)T	The command output was enhanced to display traffic indication packets (redirects).
	12.4(9)T	The <b>interface</b> and <b>tunnel</b> keywords and the <i>number</i> argument were 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.

## Examples

The following example shows output for a specific tunnel, tunnel0:

```
Router# show ip nhrp traffic interface tunnel0
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
  Sent: Total 79
        18 Resolution Request  10 Resolution Reply  42 Registration Request
         0 Registration Reply   3 Purge Request   6 Purge Reply
         0 Error Indication    0 Traffic Indication
  Rcvd: Total 69
        10 Resolution Request  15 Resolution Reply   0 Registration Request
        36 Registration Reply   6 Purge Request   2 Purge Reply
         0 Error Indication    0 Traffic Indication
```

[Table 48](#) describes the significant fields shown in the display.

**Table 48** *show ip nhrp traffic Field Descriptions*

Field	Description
Tunnel0	Interface type and number.
Max-send limit	Maximum number of NHRP messages that can be sent by this station in the given interval.
Resolution Request	Number of NHRP resolution request packets originated from or received by this station.

**Table 48** *show ip nhrp traffic Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Resolution Reply	Number of NHRP resolution reply packets originated from or received by this station.
Registration Request	Number of NHRP registration request packets originated from or received by this station.
Registration Reply	Number of NHRP registration reply packets originated from or received by this station.
Purge Request	Number of NHRP purge request packets originated from or received by this station.
Purge Reply	Number of NHRP purge reply packets originated from or received by this station.
Error Indication	Number of NHRP error packets originated from or received by this station.
Traffic Indication	Number of NHRP traffic indication packets (redirects) originated from or received by this station.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug nhrp condition</b>	Enables NHRP conditional debugging.
<b>debug nhrp error</b>	Enables NHRP error level debugging.

# show nhrp debug-condition

To display the Next Hop Resolution Protocol (NHRP) conditional debugging information, use the **show nhrp debug-condition** command in privileged EXEC mode.

**show nhrp debug-condition**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

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

**Examples** The following is sample output from the **show nhrp debug-condition** command:

```
Router# show nhrp debug-condition

Peer NBMA addresses under debug are:
1.1.1.1,
Interfaces under debug are:
Tunnel1, Peer Tunnel addresses under debug are:
2.2.2.2,
```

The output is self-explanatory. It displays the conditional debugging information for NHRP.

Related Commands	Command	Description
	<b>debug nhrp condition</b>	Enables the NHRP conditional debugging.

---

■ **show nhrp debug-condition**