show ip masks through vrf DHCP pool

show ip masks

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

show ip masks *address*

Syntax Description

address	Network address for which a mask is required.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

Command Examples

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

```
Router# show ip masks 172.16.0.0
Mask            Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip nat nvi statistics

To display NAT virtual interface (NVI) statistics, use the **show ip nat nvi statistics**command in user EXEC or privileged EXEC mode.

show ip nat nvi statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Command Examples

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

```
Router# show ip nat nvi statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended) NAT Enabled interfaces:
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0 Expired translations: 0 Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 1213 pool pool1: netmask 255.255.255.0
         start 192.168.1.10 end 192.168.1.253
         start 192.168.2.10 end 192.168.2.253
         start 192.168.3.10 end 192.168.3.253
         start 192.168.4.10 end 192.168.4.253
         type generic, total addresses 976, allocated 222 (22%), misses 0
[Id: 2] access-list 5 pool pool2 refcount 0 pool pool2: netmask 255.255.255.0
         start 192.168.5.2 end 192.168.5.254
         type generic, total addresses 253, allocated 0 (0%), misses 0
[Id: 3] access-list 6 pool pool3 refcount 3 pool pool3: netmask 255.255.255.0
         start 192.168.6.2 end 192.168.6.254
         type generic, total addresses 253, allocated 2 (0%), misses 0
[Id: 4] access-list 7 pool pool4 refcount 0 pool pool4 netmask 255.255.255.0
         start 192.168.7.30 end 192.168.7.200
         type generic, total addresses 171, allocated 0 (0%), misses 0
[Id: 5] access-list 8 pool pool5 refcount 109195 pool pool5: netmask 255.255.255.0
         start 192.168.10.1 end 192.168.10.253
         start 192.168.11.1 end 192.168.11.253
         start 192.168.12.1 end 192.168.12.253
         start 192.168.13.1 end 192.168.13.253
         start 192.168.14.1 end 192.168.14.253
         start 192.168.15.1 end 192.168.15.253
         start 192.168.16.1 end 192.168.16.253
         start 192.168.17.1 end 192.168.17.253
         start 192.168.18.1 end 192.168.18.253
         start 192.168.19.1 end 192.168.19.253
         start 192.168.20.1 end 192.168.20.253
         start 192.168.21.1 end 192.168.21.253
         start 192.168.22.1 end 192.168.22.253
         start 192.168.23.1 end 192.168.23.253
         start 192.168.24.1 end 192.168.24.253
         start 192.168.25.1 end 192.168.25.253
         start 192.168.26.1 end 192.168.26.253
         type generic, total addresses 4301, allocated 3707 (86%),misses 0 Queued Packets:
0
```

The table below describes the fields shown in the display.

Table 1: show ip nat nvi statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or timed out.
NAT enabled interfaces	List of interfaces marked as NAT enabled with the **ip nat enable** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
CEF Translated packets	Number of packets switched via Cisco Express Forwarding (CEF).
CEF Punted packets	Number of packets punted to the process switched level.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool.
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.

Field	Description
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.
Queued Packets	Number of packets in the queue.

Related Commands

Command	Description
show ip nat nvi translations	Displays active NAT virtual interface translations.

show ip nat nvi translations

To display active NAT virtual interface (NVI) translations, use the **show ip nat nvi translations** command in user EXEC or privileged EXEC mode.

show ip nat nvi translations [*protocol* [**global** | **vrf** *vrf-name*] | **vrf** *vrf-name* **| global**] **[verbose]**

Syntax Description

protocol	(Optional) Displays protocol entries. The protocol argument must be replaced with one of the following keywords: • **esp** --Encapsulating Security Payload (ESP) protocol entries. • **icmp** --Internet Control Message Protocol (ICMP) entries. • **pptp** --Point-to-Point Tunneling Protocol (PPTP) entries. • **tcp** --TCP protocol entries. • **udp** --User Datagram Protocol (UDP) entries.
global	(Optional) Displays entries in the global destination table.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Command Examples

The following is sample output from the **show ip nat nvi translations** command:

```
Router# show ip nat nvi translations
Pro    Source global       Source local       Destin  local      Destin  global
icmp   172.20.0.254:25    172.20.0.130:25      172.20.1.1:25      10.199.199.100:25
icmp   172.20.0.254:26    172.20.0.130:26      172.20.1.1:26      10.199.199.100:26
icmp   172.20.0.254:27    172.20.0.130:27      172.20.1.1:27      10.199.199.100:27
icmp   172.20.0.254:28    172.20.0.130:28      172.20.1.1:28      10.199.199.100:28
```

The table below describes the fields shown in the display.

Table 2: show ip nat nvi translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Source global	Source global address.
Source local	Source local address.
Destin local	Destination local address.
Destin global	Destination global address.

Related Commands

Command	Description
show ip nat nvi statistics	Displays NAT virtual interface statistics.

show ip nat statistics

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

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
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.

Command Examples

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

```
Router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 172.16.233.208 end 172.16.233.221
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

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

Table 3: show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is

Field	Description
	created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.

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

show ip nat translations

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

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

Syntax Description

esp	(Optional) Displays Encapsulating Security Payload (ESP) entries.
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.
pptp	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) entries.
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

Release	Modification
11.2	This command was introduced.
12.2(13)T	The **vrf** *vrf-name*keyword and argument combination was added.
12.2(15)T	The **esp** keyword was added.

Release	Modification
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.
XE 2.4.2	The **inside**and **outside**keywords were added.

Command 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 **esp** keyword:

```
Router# show ip nat translations esp

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0       192.168.122.20:0      192.168.22.20:0
```

```
192.168.22.20:28726CD9
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
```

The following is sample output that includes the **esp** and **verbose** keywords:

```
Router# show ip nat translation esp verbose

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0       192.168.122.20:0      192.168.22.20:0
192.168.22.20:28726CD9
    create 00:00:00, use 00:00:00,
    flags:
extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
    create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
    flags:
extended, use_count:0, entry-id:191, lc_entries:0
```

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 table below describes the significant fields shown in the display.

Table 4: 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.
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

Field	Description
	- 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

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

dynamic	(Optional) Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ip nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) Displays NHRP mapping entries for specified protocol addresses.
interface	(Optional) Displays NHRP mapping entries for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.
shortcut	(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 **shortcut** keyword.

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 5: Valid Types, Number Ranges, and Interface Description

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

Valid Types	Number Ranges	Interface Descriptions
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

Command 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
```

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

Table 6: 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	• 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 **ip nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.
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.
Flags	• 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. • 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. • 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

Field	Description
	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 **show ip nhrp detail** 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. • 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.
Flags (continued)	• negative--For negative caching, indicates that the requested NBMA mapping has not yet been or could not be obtained. 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. • (no socket)--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)." 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

Field	Description
	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).
Flags (continued)	• (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 . • 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. • router--Indicates that NHRP mapping entries for a remote router (that is accessing a network

Field	Description
	or host behind the remote router) are marked with the router flag. • 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 **ip nhrp registration no-unique** 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.
Flags (continued)	• 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. **Note** 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.

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
ip nhrp shortcut	Enables shortcut switching on the tunnel interface.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.
show policy-map mgre	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*]

Syntax Description

group-name	(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 (#)

Command History

Release	Modification
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.

Command 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
```

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

Table 7: 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
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show policy-map mgre	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

nbma-address	(Optional) Displays multicast mapping information for the specified NBMA address.
interface	(Optional) Displays all multicast mapping entries of the NHRP network for the interface. See the table below 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

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 8: 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

Valid Types	Number Ranges	Interface Descriptions
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
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

Command 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
```

The table below describes the fields shown in the display.

Table 9: 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	• static--Indicates that the multicast mapping entry is configured statically by the **ip nhrp map multicast** command.

Field	Description
	- 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 **ip nhrp map multicast dynamic** command is configured.

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 nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	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*] **[detail]**

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.

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.

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 10: 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

Valid Types	Number Ranges	Interface Descriptions
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
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

Command 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:
  5.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 5.1.1.1
```

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

Table 11: 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 nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	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.

Command 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
```

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

Table 12: 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 **ip nhrp map** command are marked static.
incomplete	NBMA address is not known for the target network.

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 nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp traffic	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 *number*	(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 show output was enhanced to display information about traffic indication (redirects).
12.4(9)T	The **interface** and **tunnel** keywords and the *number* 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.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Command 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
```

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

Table 13: 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.
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

Command	Description
debug nhrp condition	Enables NHRP conditional debugging.
debug nhrp error	Enables NHRP error level debugging.

show ip route dhcp

To display the routes added to the routing table by the Dynamic Host Configuration Protocol (DHCP) server and relay agent, use the **show ip route dhcp** command in privileged EXEC configuration mode.

show ip route [**vrf** *vrf-name*] **dhcp** [*ip-address*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be displayed.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

To display information about global routes, use the **show ip route dhcp** command. To display routes in the VRF routing table, use the **show ip route vrf** *vrf-name* **dhcp** command.

Command Examples

The following is sample output from the **show ip route dhcp**command when entered without an address. This command lists all routes added by the DHCP server and relay agent.

```
Router# show ip route dhcp
```

```
  10.5.5.56/32 is directly connected, ATM0.2
  10.5.5.217/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route dhcp** command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route dhcp 10.5.5.217

  10.5.5.217 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 01:19 PM
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when entered without an address:

```
Router# show ip route vrf abc dhcp
  10.5.5.218/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route vrf red dhcp 10.5.5.218
  10.5.5.218/32 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

Related Commands

Command	Description
clear ip route dhcp	Removes routes from the routing table added by the DHCP server and relay agent for the DHCP clients on unnumbered interfaces.

show ip snat

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

show ip snat [**distributed [verbose]** | **peer** *ip-address*]

Syntax Description

distributed	(Optional) Displays information about the distributed NAT, including its peers and status.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
peer *ip-address*	(Optional) Displays TCP connection information between peer routers.

Command Modes

EXEC

Command History

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

Command Examples

The following is sample output from the **show ip snat distributed** command for stateful NAT connected peers:

```
Router# show ip snat distributed
Stateful NAT Connected Peers
SNAT: Mode PRIMARY
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
```

The following is sample output from the **show ip snat distributed verbose**command for stateful NAT connected peers:

```
Router# show ip snat distributed verbose
SNAT: Mode PRIMARY
Stateful NAT Connected Peers
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
```

```
:Mapping List 10
:InMsgs 7, OutMsgs 7, tcb 0x63EBA408, listener 0x0
```

show ip source binding

To display IP-source bindings configured on the system, use the **show ip source command** command in privileged EXEC mode.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping | static**] [**vlan** *vlan-id*] [**interface** *type mod*/*port*]

Syntax Description

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

Command Default

Both static and DHCP-snooping bindings are displayed.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Each optional parameter is used to filter the display output.

Command Examples

This example shows the output without entering any keywords:

Router# **show ip source binding**

```
MacAddress              IpAddress        Lease(sec) Type          VLAN Interface
```

```
------------------     --------------- ---------- ------------ ---- --------------------
00:00:00:0A:00:0B      17.16.0.1        infinite   static        10   FastEthernet6/10
00:00:00:0A:00:0A      17.16.0.2        10000      dhcp-snooping 10   FastEthernet6/11
```

This example shows how to display the static IP binding entry for a specific IP address:

```
Router# show ip source binding 17.16.0.1 0000.000A.000B static vlan 10 interface
gigabitethernet6/10
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:00:00:0A:00:0B   17.16.0.1         infinite    static         10    FastEthernet6/10
```

The table below describes the significant fields in the display.

Table 14: show ip source binding Field Descriptions

Field	Description
MAC Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; static bindings configured from CLI to dynamic binding learned from DHCP snooping.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per 12-port IP source guard.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

show ip verify source

To display the IP source guard configuration and filters on a particular interface, use the **show ip verify source** command in EXEC mode.

show ip verify source [**interface** *type mod*/*port*] [**efp_id efp_id**]

Syntax Description

interface *type*	(Optional) Specifies the interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.
efp_id	(Optional) Specifies the Ethernet flow point (EFP) (service instance) ID.
efp_id	EFP number; range is 1 to 8000.

Command Default

This command has no default settings.

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **efp_id** *efp_id*keyword and argument were added.

Usage Guidelines

Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

Command Examples

This example shows the display when DHCP snooping is enabled on VLANs 10 to 20, the interface has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

```
Router# show ip verify source interface gigabitethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
```

```
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                                11-20
```

This example shows how to display the IP source guard configuration and filters on a specific interface:

```
Router# show ip verify source interface gigabitethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           inactive-trust-port
```

This example shows the display when the interface does not have a VLAN enabled for DHCP snooping:

```
Router# show ip verify source interface gigabitethernet6/3
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/3      ip           inactive-no-snooping-vlan
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 10.0.0.1/aaaa.bbbb.cccd on VLAN 11:

```
Router# show ip verify source interface gigabitethernet6/4
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       10.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binding 10.0.0.3/aaaa.bbbb.ccce on VLAN 10, but port security is not enabled on the interface:

```
Router# show ip verify source interface gigabitethernet6/5
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
```

This example shows the display when the interface does not have IP source filter mode configured:

```
Router# show ip verify source interface gigabitethernet6/6
DHCP security is not configured on the interface gi6/6.
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                         11-20
gi6/2      ip           inactive-trust-port
gi6/3      ip           inactive-no-snooping-vlan
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
Router#
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source interface gi5/0/0 efp_id 10
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan        EFP
ID
```

```
---------    -----------    -----------      ---------------     -----------------
----------  ----------
Gi5/0/0    ip-mac       active          123.1.1.1        00:0A:00:0A:00:0A  100
10
Gi5/0/0    ip-mac       active          123.1.1.2        00:0A:00:0A:00:0B  100
20
Gi5/0/0    ip-mac       active          123.1.1.3        00:0A:00:0A:00:0C  100
30
```

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per l2-port IP source guard.
show ip source binding	Displays the IP-source bindings configured on the system.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list** command in privileged EXEC mode.

show logging ip access-list {**cache** | **config**}

Syntax Description

cache	Displays information about all the entries in the Optimized ACL Logging (OAL) cache.
config	Displays information about the logging IP access-list configuration.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the **config** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

Command Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 10.2.1.82 10.2.12.2 111 63 Permit 0
```

```
3906 2d02h
2 17 10.2.1.82 10.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 10.2.1.82 10.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 10.2.1.82 10.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 10.2.1.82 10.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 10.2.1.82 10.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 10.2.1.82 10.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 10.2.1.82 10.2.12.2 7279 63 Permit 0
3906 2d02h
9 17 10.2.1.82 10.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 10.2.1.82 10.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 10.2.1.82 10.2.12.2 10351 63 Permit 0
3905 2d02h
12 17 10.2.1.82 10.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 10.2.1.82 10.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 10.2.1.82 10.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 10.2.1.82 10.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 10.2.1.82 10.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 10.2.1.82 10.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 10.2.1.82 10.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 10.2.1.82 10.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 10.2.1.82 10.2.12.2 19567 63 Permit 0
3905 2d02h
Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config
Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.

Command	Description
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.

show nat64 adjacency

To display information about the stateless Network Address Translation 64 (NAT64) managed adjacencies, use the **show nat64 adjacency** command in user EXEC or privileged EXEC mode.

show nat64 adjacency {**all** | **count** | **ipv4** | **ipv6**}

Syntax Description

all	Displays all adjacencies.
count	Displays the adjacency count.
ipv4	Displays IPv4 adjacencies.
ipv6	Displays IPv6 adjacencies.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

An adjacency is a node that can be reached by one Layer 2 hop. The stateless NAT64 adjacencies include adjacency addresses and the total number of adjacencies.

Command Examples

The following is sample output from the **show nat64 adjacency all** command:

```
Router# show nat64 adjacency all

Adjacency Counts
 IPv4 Adjacencies: 2
 IPv6 Adjacencies: 1
 Stateless Prefix Adjacency Ref Count: 1
Adjacencies
 IPv6 Adjacencies
    ::42
 IPv4 Adjacencies
    0.0.19.137 (5001)
    0.0.19.140 (5004)
```

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

Table 15: show nat64 adjacency all Field Descriptions

Field	Description
Adjacency Counts	Count of all adjacencies.
Adjacencies	Types of adjacencies.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 ha status

To display information about the stateless Network Address Translation 64 (NAT64) high availability (HA) status, use the **show nat64 ha status**command in user EXEC or privileged EXEC mode.

show nat64 ha status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Command Examples

The following is sample output from the **show nat64 ha status** command:

```
Router# show nat64 ha status
NAT64 HA Status
 Role: active
 Peer is ready: TRUE
 Peer is compatible: TRUE
 Synchronization enabled: TRUE
 Is hot (standby): FALSE
 Bulk sync PID: NO_PROCESS
 ISSU negotiation status: IPC, CF
 ISSU context IDs: IPC(198), CF(197)
 Synchronization capabilities: 0x00000001
  Adjacency mappings: TRUE
 CF info: handle(0x0000011B), peer ready(TRUE),
  flow control(TRUE)(FALSE)(0x0)
 Initialized: HA(TRUE) ISSU(TRUE)
 Message stats:
  Adjacency mapping: rx(0) tx(5001) tx err(0)
  Bulk sync done: rx(0) tx(1) tx err(0)
 Errors:
  Bulk sync: 0
  CF tx: 0
```

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

Table 16: show nat64 ha status Field Descriptions

Field	Description
NAT64 HA Status	Status of stateless NAT64 HA.
Message stats	Status of the messages.

Field	Description
Errors	Types of errors.

Related Commands

Command	Description
clear nat64 ha statistics	Clears stateless NAT64 HA statistics.
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 prefix stateless

To display information about the configured Network Address Translation 64 (NAT64) stateless prefixes, use the **show nat64 prefix stateless**command in user EXEC or privileged EXEC mode.

show nat64 prefix stateless {**global** | {**interfaces | static-routes**} [**prefix** *ipv6-prefix*/*prefix-length*]}

Syntax Description

global	Displays the global stateless prefixes.
interfaces	Displays the interfaces and the stateless prefixes used by the interfaces.
prefix	(Optional) Displays the interfaces that are using a specific stateless prefix.
static-routes	Displays the static routes that are using the stateless prefix.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	(Optional) Length of the IPv6 prefix. Prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Valid values are from 0 to 128.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The output of the **show nat64 prefix stateless** command displays the interfaces that use a specific prefix and the number of prefixes that use a static route.

Command Examples

The following is sample output from the **show nat64 prefix stateless global**command:

```
Router# show nat64 prefix stateless global
Global Prefix: is valid, 2001::/96
IFs Using Global Prefix
   Fa0/3/4
   Fa0/3/5
```

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

Table 17: show nat64 prefix stateless global Field Descriptions

Field	Description
Global Prefix	IPv6 stateless prefix configured at the global level.
IFs Using Global Prefix	Lists the interfaces that are using the specified global prefix.

The following is sample output from the **show nat64 prefix stateless interfaces**command.

```
Router# show nat64 prefix stateless interfaces

Interface           NAT64 Enabled    Global    Stateless Prefix
FastEthernet0/3/4   TRUE             FALSE     2001::/96
```

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

Table 18: show nat64 prefix stateless interfaces Field Descriptions

Field	Description
Interface	Interface name and number.
NAT64 Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Global	Information on whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.
Stateless Prefix	Stateless prefix used for NAT64 translation.

The following is sample output from the **show nat64 prefix stateless static-routes**command. The output fields are self-explanatory.

```
Router# show nat64 prefix stateless static-routes

Stateless            Prefix Static Route Ref Count
2001::/96               1
```

Related Commands

Command	Description
nat64 prefix	Assigns a global or interface-specific NAT64 stateless prefix.

show nat64 routes

To display information about the configured Network Address Translation 64 (NAT64) routes, use the **show nat64 routes**command in privileged EXEC mode.

show nat64 routes [**adjacency** *address* | **interface** *type number* | **prefix** *prefix-length*]

Syntax Description

adjacency	(Optional) Displays the route for an adjacency address.
address	(Optional) Adjacency address for lookup.
interface	(Optional) Displays routes pointing to an 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.
prefix	(Optional) Displays the route of an IPv4 prefix.
prefix-length	(Optional) Length of the IPv4 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The output of the **show nat64 routes** command displays the stateless prefix and adjacency used by the routes and information on whether the routes are enabled.

Command Examples

The following is sample output from the **show nat64 routes** command:

```
Router# show nat64 routes
IPv4 Prefix          Adj. Address    Enabled   Output IF    Global    IPv6 Prefix
```

```
192.0.2.1/24          0.0.19.137      FALSE     Fa0/3/4
198.51.100.253/24     0.0.19.140      TRUE      Fa0/3/0      FALSE     3001::/96
```

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

Table 19: show nat64 routes Field Descriptions

Field	Description
IPv4 Prefix	Prefix used by IPv4 address.
Adj. Address	Adjacency address.
Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Output IF	Output interfaces.
Global	Information on whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.

show nat64 statistics

To display Network Address Translation 64 (NAT64) packet count statistics, use the **show nat64 statistics**command in user EXEC or privileged EXEC mode.

show nat64 statistics [**global** | **interface** *type number* | **prefix** *ipv6-prefix*/*prefix-length*]

Syntax Description

global	(Optional) Displays global NAT64 statistics.
interface	(Optional) Displays statistics for an 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.
prefix	(Optional) Displays statistics for a specified prefix.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. The valid values are from 0 to 128.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The output of the **show nat64 statistics** command displays the interfaces configured for stateless NAT64 and the packets that were translated or dropped.

Command Examples

The following is sample output from the **show nat64 statistics** command:

```
Router# show nat64 statistics
NAT64 Statistics
Global Stats:
   Packets translated (IPv4 -> IPv6): 21
   Packets translated (IPv6 -> IPv4): 15
GigabitEthernet0/0/1 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 5
   Packets translated (IPv6 -> IPv4): 0
   Packets dropped: 0
GigabitEthernet1/2/0 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 0
   Packets translated (IPv6 -> IPv4): 5
   Packets dropped: 0
```

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

Table 20: show nat64 statistics Field Descriptions

Field	Description
Global Stats	Statistics of all the NAT64 interfaces.
Packets translated	Number of packets translated from IPv4 to IPv6 and vice versa.
Packets dropped	Number of packets dropped. The packets that are not translated are dropped.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

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.

Command 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 if self-explanatory. It displays the conditional debugging information for NHRP.

Related Commands

Command	Description
debug nhrp condition	Enables the NHRP conditional debugging.

show platform hardware qfp feature

To display feature-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature**command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature alg** {**memory** | **statistics** [*protocol* | **clear [clear]**]}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
alg	Displays the Application Level Gateway (ALG) information of the processor.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.
protocol	Protocol name. It can be one of the following values: • **dns** --Displays Domain Name System (DNS) ALG information in the QFP datapath. • **exec** --Displays exec ALG information in the QFP datapath. • **ftp** --Displays FTP ALG information in the QFP datapath. • **h323** --Displays H.323 ALG information in the QFP datapath. • **http** --Displays HTTP ALG information in the QFP datapath. • **imap** --Displays Internet Message Access Protocol (IMAP) ALG information in the QFP datapath. • **ldap** --Displays Lightweight Directory Access Protocol (LDAP) ALG information in the QFP datapath. • **login** --Displays login ALG information in the QFP datapath. • **netbios** --Displays Network Basic Input Output System (NetBIOS) ALG information in the QFP datapath. • **pop3** --Displays pop3 ALG information in the QFP datapath.

	• **rtsp** --Displays Rapid Spanning Tree Protocol (RSTP) ALG information in the QFP datapath. • **shell** --Displays shell ALG information in the QFP datapath. • **sip** --Displays Session Initiation Protocol (SIP) ALG information in the QFP datapath. • **skinny** --Displays skinny ALG information in the QFP datapath. • **smtp** --Displays Simple Mail Transfer Protocol (SMTP) ALG information in the QFP datapath. • **sunrpc** --Displays Sun RPC ALG information in the QFP datapath. • **tftp** --Displays TFTP ALG information in the QFP datapath.
clear	(Optional) Clears ALG common counters after display.
clear	(Optional) Clears the ALG counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the NetBIOS protocol was added.
Cisco IOS XE Release 3.2S	This command was modified. The show output was modified to display SIP statistics information.

Usage Guidelines

The **show platform hardware qfp feature** command when used withthe **netbios** keyworddisplays the NetBIOS ALG memory usage and statistics information of the processor.

Command Examples

The following example displays the NetBIOS ALG statistics information of the processor:

```
Router# show platform hardware qfp active feature alg statistics netbios
NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0  No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets            :0
    Direct unique packets    :0
    Direct group packets     :0
    Broadcast packets        :0
    DGM Error packets        :0
    Query request packets    :0
    Positive Qry response packets :0
    Netgative Qry response packets:0
    Unknown packets          :0
    Total error packets      :0
  Name Service statistics
    Total packets            :0
    Query request packets    :0
    Query response packets   :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets  :0
    Release response packets :0
    WACK packets             :0
    Refresh packets          :0
    Unknown packets          :0
    Total error packets      :0
  Session Service statistics
    Total packets            :0
    Message packets          :0
    Request packets          :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets        :0
    Unknown packets          :0
    Total error packets      :0
```

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

Table 21: show platform hardware qfp feature Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Number of direct unique NetBIOS packets processed.
Direct group packets	Number of direct group NetBIOS packets processed.
Broadcast packets	Number of broadcast NetBIOS packets processed.
DGM Error packets	Number of Datagram Error NetBIOS packets processed.
Query request packets	Number of query request NetBIOS packets processed.
Positive Qry response packets	Number of positive query response NetBIOS packets processed.

Field	Description
Negative Qry response packets	Number of negative query response NetBIOS packets processed.
Unknown packets	Number of unknown packets.
Total error packets	Counter tracking number of error packets.

The following example displays SIP statistics information of the processor. The field descriptions are self-explanatory.

```
Router# show platform hardware qfp active feature alg statistics sip
SIP info pool used chunk entries number: 0
RECEIVE
Register: 0 -> 200-OK: 0
Invite: 0 -> 200-OK: 0 Re-invite 0
Update: 0 -> 200-OK: 0
Bye: 0 -> 200-OK: 0
Trying: 0 Ringing: 0 Ack: 0
Info: 0 Cancel: 0 Sess Prog: 0
Message: 0 Notify: 0 Prack: 0
OtherReq: 0 OtherOk: 0
Events
Null dport: 0 Media Port Zero: 0
Malform Media: 0 No Content Length: 0
Cr Trunk Chnls: 0 Del Trunk Chnls: 0
Cr Normal Chnls: 0 Del Normal Chnls: 0
Media Addr Zero: 0 Need More Data: 0
Errors
Create Token Err: 0 Add portlist Err: 0
Invalid Offset: 0 Invalid Pktlen: 0
Free Magic: 0 Double Free: 0
Retmem Failed: 0 Malloc Failed: 0
Bad Format: 0 Invalid Proto: 0
Add ALG state Fail: 0 No Call-id: 0
Parse SIP Hdr Fail: 0 Parse SDP Fail: 0
Error New Chnl: 0 Huge Size: 0
Create Failed: 0
Writeback Errors
Offset Err: 0 PA Err: 0
No Info: 0
```

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs feature-specific information in the QFP.

show platform software trace message

To display trace messages for a module, enter the **show platform software trace message** command in privileged EXEC mode or diagnostic mode.

show platform software trace message *process hardware-module slot*

Syntax Description

process	The process in which the tracing level is being set. The following keywords are available: • **chassis-manager** --The Chassis Manager process. • **cpp-control-process** --The Cisco packet processor (CPP) Control process. • **cpp-driver** --The CPP driver process. • **cpp-ha-server** --The CPP high availability (HA) server process. • **cpp-service-process** --The CPP service process. • **forwarding-manager** --The Forwarding Manager process. • **host-manager** --The Host Manager process. • **interface-manager** --The Interface Manager process. • **ios** --The Cisco IOS process. • **logger** --The logging manager process. • **pluggable-services** --The pluggable services process. • **shell-manager** --The Shell Manager process.
hardware-module	Tthe hardware module where the process whose trace level is being set is running. The following keywords are available: • **carrier-card** --The process is on an SPA Interface Processor (SIP). • **forwarding-processor** --The process is on an embedded services processor (ESP). • **route-processor** --The process is on an route processor (RP).
slot	The slot of the hardware module. Options are as follows: • *number* --The number of the SIP slot of the hardware module where the trace level is being

	set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2. • *SIP-slot* **/** *SPA-bay* --The number of the SIP router slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active** --The CPP in the active ESP. • **cpp standby** --The CPP in the standby ESP. • **f0** --The ESP in ESP slot 0. • **f1** --The ESP in ESP slot 1 • **fp active** --The active ESP. • **fp standby** --The standby ESP.
	• **r0** --The RP in RP slot 0. • **r1** --The RP in RP slot 1. • **rp active** --The active RP. • **rp standby** --The standby RP. • **qfp active** --The active Quantum Flow Processor (QFP)

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
12.2(33)XND	This command was modified. The command output displays the truncated traceback message also.
Cisco IOS XE Release XE 3.1S	The **qfp active** keywords were added.

Usage Guidelines

The **show platform software trace message** command is used to display trace messages from an in-memory message ring of a module’s process that keeps a condensed historical record of all messages. Although all messages are saved in a trace log file unmodified, only the first 128 bytes of a message are saved in the message ring. The size limitation does not apply to the traceback portion of a message.

Command Examples

The following example shows how to display the trace messages for the Host Manager process in RP slot 0 using the **show platform software trace message** command:

```
Router# show platform software trace message host-manager R0
```

```
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager
in slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager
in slot 0
```

The following example shows a truncated message that has a traceback. The truncated portion of the message is indicated by an ellipsis (...):

```
03/02 15:47:44.002 [errmsg]: (ERR): %EVENTLIB-3-TIMEHOG: read asyncon 0x100a9260:
60618ms,
Traceback=1#862f8780825f93a618ecd9 ...Traceback=1#862f8780825f93a618ecd9dd48b3be96
evlib:FCAF000+CC00 evlib:FCAF000+A6A8 evutil:FFCA000+ADD0 evutil:FFCA000+5A80
evutil:FFCA000+A68C uipeer:FF49000+10AFC evlib:FCAF000+D28C evlib:FCAF000+F4C4 :
10000000+1B24C c:EF44000+1D078 c:EF44000+1D220
```

Related Commands

Command	Description
set platform software trace	Sets the trace level for a specific module.
show platform software trace levels	Displays trace levels for a module.

show redundancy application control-interface group

To display control interface information for a redundancy group, use the **show redundancy application control-interface group**command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application control-interface**command shows information for the redundancy group control interfaces.

Command Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application data-interface

To display data interface-specific information, use the **show redundancy application data-interface**command in privileged EXEC mode.

show redundancy application data-interface group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application data-interface**command displays information about the redundancy group data interfaces.

Command Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

Command	Description
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application faults group

To display fault-specific information for a redundancy group, use the **show redundancy application faults group**command in privileged EXEC mode.

show redundancy application faults group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application faults**command shows information returned by redundancy group faults.

Command Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
```

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

Table 22: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group. This field is important when monitoring redundancy group switchover and when configuring interface tracking.

Field	Description
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group**command in privileged EXEC mode.

show redundancy application group [*group-id* | **all**]

Syntax Description

group-id	(Optional) redundancy group ID. Valid values are 1 and 2.
all	(Optional) Display the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **show redundancy application group**command to display the current state of each interbox redundancy group on the device and the peer device.

Command Examples

The following is sample output from the **show redundancy application group all** command:

```
Router# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0
RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 2
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0
RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Standby Peer: Not Present.
```

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

Table 23: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	The redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	The current role of the device.
Peer Role	The current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer box has started RF progression.
RF Domain	The name of RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

Command	Description
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr**command in privileged EXEC mode.

show redundancy application if-mgr group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application if-mgr**command shows information of traffic interfaces protected by redundancy groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Command Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2
RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 ==========================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

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

Table 24: show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.

Field	Description
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.
Shut	The state of this interface. **Note** It is always “shut” on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application protocol	Displays protocol-specific information for a redundancy group

show redundancy application protocol

To display protocol-specific information for a redundancy group, use the **show redundancy application protocol**command in privileged EXEC mode.

[1]

Syntax Description

protocol-id	Protocol ID. The range is from 1 to 8.
group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application protocol**command shows information returned by redundancy group protocol.

Command Examples

The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
 BFD: ENABLE
 Hello timer in msecs: 0
 Hold timer in msecs: 0
```

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

Table 25: show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.

[1]

Field	Description
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msecs	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msecs.
Hold timer in msecs	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msecs.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport-specific information for a redundancy group, use the **show redundancy application transport**command in privileged EXEC mode.

show redundancy application transport {**client** | **group** [*group-id*]}

Syntax Description

client	Displays transport client-specific information.
group	Displays the redundancy group name.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application transport**command shows information for redundancy group transport.

Command Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.

Command	Description
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

snmp-server enable traps dhcp

To enable DHCP Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps dhcp** command in global configuration mode. To disable DHCP trap notifications, use the **no** form of this command.

snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

no snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Command Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

```
Router(config)# snmp-server enable traps dhcp
```

subnet prefix-length

To configure a subnet allocation pool and determine the size of subnets that are allocated from the pool, use the **subnet prefix-length** command in DHCP pool configuration mode. To unconfigure subnet pool allocation, use the **no** form of this command.

subnet prefix-length *prefix-length*

no subnet prefix-length *prefix-length*

Syntax Description

prefix-length	Configures the IP subnet prefix length in classless interdomain routing (CIDR) bit count notation. The range is from 1 to 31.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is used to configure a Cisco IOS router as a subnet allocation server for a centralized or remote Virtual Private Network (VPN) on-demand address pool (ODAP) manager. This command is configured under a DHCP pool. The *prefix-length* argument is used to determine the size of the subnets that are allocated from the subnet allocation pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format.

Configuring Global Subnet Pools

Global subnet pools are created in a centralized network. The ODAP server allocates subnets from the subnet allocation server based on subnet availability. When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP server requires the address space. The binding is destroyed and the subnet is returned to the subnet pool only when the ODAP server releases the subnet as address space utilization decreases.

Configuring VPN Subnet Pools

A subnet allocation server can be configured to assign subnets from VPN subnet allocation pools for Multiprotocol Label Switching (MPLS) VPN clients. VPN routes between the ODAP manager and the subnet allocation server are configured based on VRF name or VPN ID configuration. The VRF and VPN ID are configured to maintain routing information that defines customer VPN sites. This customer site is attached to a provider edge (PE) router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

Configuring VPN Subnet Pools for VPN clients with VPN IDs

A subnet allocation server can also be configured to assign subnets from VPN subnet allocation pools based on the VPN ID of a client. The VPN ID (or Organizational Unique Identifier [OUI]) is a unique identifier assigned by the IEEE. VPN routes between the ODAP manager and the subnet allocation server are enabled by configuring the DHCP pool with a VPN ID that matches the VPN ID that is configured for the VPN client.

Command Examples

Examples

The following example configures a router to be a subnet allocation server and creates a global subnet allocation pool named GLOBAL-POOL from the 10.0.0.0 network. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 254 host IP addresses.

```
ip dhcp pool GLOBAL-POOL
 network 10.0.0.0 255.255.255.0
 subnet prefix-length 24
```

Examples

The following example configures a router to be a subnet allocation server and creates a VPN routing and forwarding (VRF) subnet allocation pool named VRF-POOL from the 172.16.0.0 network and configures the VPN to match the VRF named pool1. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 62 host IP addresses.

```
ip dhcp pool VRF-POOL
  vrf pool1
 network 172.16.0.0 /16
 subnet prefix-length 26
```

Examples

The following example configures a router to be a subnet allocation server and creates a VRF subnet allocation pool named VPN-POOL from the 192.168.0.0 network and configures the VRF named abc. The VPN ID must match the unique identifier that is assigned to the client site. The route target and route distinguisher are configured in the as-number:network number format. The route target and route distinguisher must match. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 30 host IP addresses.

```
ip vrf abc
 rd 100:1
 route-target both 100:1
 vpn id 1234:123456
!
ip dhcp pool VPN-POOL
 vrf abc
 network 192.168.0.0 /24
 subnet prefix-length /27
```

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
ip dhcp pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
show ip dhcp pool	Displays information about the DHCP pools.

term ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format**command inEXEC configuration mode. To restore the default display format, use the **no** form of this command.

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

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

Syntax Description

bitcount	Number of bits in the netmask.
decimal	Netmask dotted decimal notation.
hexadecimal	Netmask hexadecimal format.

Command Default

Netmasks are displayed in dotted decimal format.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0XFFFFFF00.

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

Command Examples

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

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

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime**command in redundancy application protocol configuration mode. To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [msec] *seconds* **holdtime [msec]** *seconds*

no timers hellotime [msec] *seconds* **holdtime [msec]** *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages.
seconds	Interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application protocol configuration (config-red-app-prtc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Command Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

update arp

To secure dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings, use the **update arp**command in DHCP pool configuration mode. To disable this command and change secure ARP entries to dynamic ARP entries, use the **no** form of this command.

update arp

no update arp

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

The **update arp** DHCP pool configuration command is used to secure ARP table entries and their corresponding DHCP leases. However, existing active leases are not secured. These leases will remain insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

This command can be configured only under the following conditions:

- DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- Directly connected clients on LAN interfaces and wireless LAN interfaces.

The configuration of this command is not visible to the client. When this command is configured, secured ARP table entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior. If a secure ARP entry created by the DHCP server must be removed, the **clear ip dhcp binding** command can be used. This command will clear the DHCP binding and secured ARP table entry.

Note This command does not secure ARP table entries for BOOTP clients.

Command Examples

The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
ip dhcp pool WIRELESS-POOL
 update arp
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP Server database.

update dns

To dynamically update the Domain Name System (DNS) with address (A) and pointer (PTR) Resource Records (RRs) for some address pools, use the **update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

update dns [**both** | **never**] **[override] [before]**

no update dns [**both** | **never**] **[override] [before]**

Syntax Description

both	(Optional) Dynamic Host Configuration Protocol (DHCP) server will perform Dynamic DNS (DDNS) updates for both PTR (reverse) and A (forward) RRs associated with addresses assigned from an address pool.
never	(Optional) DHCP server will not perform DDNS updates for any addresses assigned from an address pool.
override	(Optional) DHCP server will perform DDNS updates for PTR RRs associated with addresses assigned from an address pool, even if the DHCP client has specified in the fully qualified domain name (FQDN) option that the server should not perform updates.
before	(Optional) DHCP server will perform DDNS updates before sending the DHCP ACK back to the client. The default is to perform updates after sending the DHCP ACK.

Command Default

No updates are performed.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines

If you configure the **update dns both override** command, the DHCP server will perform DDNS updates for both PTR and A RRs associated with addresses assigned from an address pool, even if the DHCP client specified in the FQDN that the server should not.

If the server is configured using this command with or without any of the other keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and act as though it were configured to update both A and PTR records on behalf of the client.

Command Examples

The following example shows how to configure the DHCP to never update the A and PTR RRs:

```
update dns never
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

utilization mark high

To configure the high utilization mark of the current address pool size, use the **utilization mark high** command in DHCP pool configuration mode. To remove the high utilization mark, use the **no** form of this command.

utilization mark high *percentage-number* **[log]**

no utilization mark high *percentage-number* **[log]**

Syntax Description

percentage-number	Percentage of the current pool size.
log	(Optional) Enables the logging of a system message.

Command Default

The default high utilization mark is 100 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(4)T	The **log** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level exceeds the configured high utilization mark, the pool will schedule a subnet request.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Command Examples

The following example sets the high utilization mark to 80 percent of the current pool size:

```
utilization mark high 80
```

The following pool configuration using the **log** keyword option generates a system message:

```
! ip dhcp pool abc
utilization mark high 30 log
utilization mark low 25 log
network 10.1.1.0 255.255.255.248
!
```

The following system message is generated when the second IP address is allocated from the pool:

```
00:02:01: %DHCPD-6-HIGH_UTIL: Pool "abc" is in high utilization state (2 addresses used
out of 6). Threshold set at 30%.
```

The following system message is generated when one of the two allocated IP addresses is returned to the pool:

```
00:02:58: %DHCPD-6-LOW_UTIL: Pool "abc" is in low utilization state (1 addresses used out
of 6). Threshold set at 25%.
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark low	Configures the low utilization mark of the current address pool size.

utilization mark low

To configure the low utilization mark of the current address pool size, use the **utilization mark low** command in DHCP pool configuration mode. To remove the low utilization mark, use the **no** form of this command.

utilization mark low *percentage-number*

no utilization mark low *percentage-number*

Syntax Description

percentage-number	Percentage of the current pool size.

Command Default

The default low utilization mark is 0 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level drops below the configured low utilization mark, a subnet release is scheduled from the address pool.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Command Examples

The following example sets the low utilization mark to 20 percent of the current pool size:

```
utilization mark low 20
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark high	Configures the high utilization mark of the current address pool size.

view (DNS)

To access or create the specified Domain Name System (DNS) view list member in the DNS view list and then enter DNS view list member configuration mode, use the **view** command in DNS view list configuration mode. To remove the specified DNS view list member from the DNS view list, use the **no** form of this command.

view [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*

no view [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is added to the view list anyway. The specified VRF can be defined after the view is added as a member of the view list (and after the view itself is defined). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
default	Specifies that the DNS view is unnamed. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
view-name	String (not to exceed 64 characters) that identifies the name of an existing DNS view. **Note** If the specified view does not exist, a warning is displayed but the default view list member is added anyway. The specified view can be defined after it is added as a member of DNS view list. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
order-number	Integer from 1 to 2147483647 that specifies the order in which the DNS view is checked, with

respect to other DNS views in the same DNS view list.

Tip If the *order-number* values for the DNS views within a DNS view list are configured with large intervals between them (for example, by specifying *order-number* values such as 10, 20, and 30), additional DNS views can be inserted into the view list quickly without affecting the existing ordering or views in the view list. That is, adding a new view to the view list--or changing the ordering of existing views within the view list--does not require that existing views in the view list be removed from the view list and then added back to the list with new *order-number* values.

Command Default

No DNS view is accessed or created.

Command Modes

DNS view list configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enters DNS view list member configuration mode--for the specified view list member--so that usage restrictions can be configured for that view list member. If the DNS view list member does not exist yet, the specified DNS view is added to the DNS view list along with the value that indicates the order in which the view list member is to be checked (relative to the other DNS views in the view list) whenever the router needs to determine which DNS view list member to use to address a DNS query.

Note The maximum number of DNS views and view lists supported is not specifically limited but is dependent on the amount of memory on the Cisco router. Configuring a larger number of DNS views and view lists uses more router memory, and configuring a larger number of views in the view lists uses more router processor time. For optimum performance, configure no more views and view list members than needed to support your Split DNS query forwarding or query resolution needs.

Note

The parameters {**default** | *view-name*} and [**vrf** *vrf-name*] identify an existing DNS view, as defined by using the **ip dns view** command. More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

The **view** command can be entered multiple times to specify more than one DNS view in the DNS view list.

To display information about a DNS view list, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List Member

After you use the **view** command to define a DNS view list member and enter DNS view list member configuration mode, you can use any of the following commands to configure usage restrictions for the DNS view list member:

- **restrict authenticated**
- **restrict name-group**
- **restrict source access-group**

These optional, additional restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively. If none of these optional restrictions are configured for the view list member, the only usage restriction on the view list member is the usage restriction based on its association with a VRF.

Reordering of DNS View List Members

To provide for efficient management of the order of the members in a view list, each view list member definition includes the specification of the position of that member within the list. That is, the order of the members within a view list is defined by explicit specification of position values rather than by the order in which the individual members are added to the list. This enables you to add members to an existing view list or reorder the members within an existing view list without having to remove all the view list members and then redefine the view list membership in the desired order:

Command Examples

The following example shows how to add the view user3 to the DNS view list userlist5 and assign this view member the order number 40 within the view list. Next, the view user2, associated with the VRF vpn102 and assigned the order number 20 within the view list, is removed from the view list.

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# exit

Router(cfg-dns-view-list)# no view vrf vpn102 user2 20
```

Related Commands

Command	Description
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.

Command	Description
restrict authenticated	Restricts the use of the DNS view list member to DNS queries for which the DNS query host can be authenticated.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

vrf (DHCP pool)

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

name	Name of the VRF to which the address pool is associated.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Associating a pool with a VRF allows overlapping addresses with other pools that are not on the same VRF. Only one pool can be associated with each VRF. If the pool is configured with the **origin dhcp** command or **origin aaa** command, the VRF information is sent in the subnet request. If the VRF is configured with an RFC 2685 VPN ID, the VPN ID will be sent instead of the VRF name.

Command Examples

The following example associates the on-demand address pool with a VRF named pool1:

```
ip dhcp pool pool1
  origin dhcp subnet size initial 24 autogrow 24
  utilization mark high 85
  utilization mark low 15
  vrf pool1
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.