

show ip masks through vrf DHCP pool

- show ip masks, on page 4
- show ip nat limits all-host, on page 5
- show ip nat limits all-vrf, on page 7
- show ip nat nvi statistics, on page 9
- show ip nat nvi translations, on page 11
- show ip nat redundancy, on page 13
- show ip nat statistics, on page 15
- show ip nat statistics platform, on page 17
- show ip nat translations, on page 19
- show ip nat translation entry-id platform, on page 23
- show ip nat translations redundancy, on page 24
- show ip nhrp, on page 25
- show ip nhrp group-map, on page 36
- show ip nhrp multicast, on page 38
- show ip nhrp multicast stats, on page 41
- show ip nhrp nhs, on page 42
- show ip nhrp redirect, on page 45
- show ip nhrp summary, on page 47
- show ip nhrp traffic, on page 48
- show ip route dhcp, on page 50
- show ip snat, on page 52
- show ip source binding, on page 53
- show ip verify source, on page 55
- show ipv6 dhcp, on page 58
- show ipv6 dhcp binding, on page 59
- show ipv6 dhcp conflict, on page 62
- show ipv6 dhcp database, on page 63
- show ipv6 dhcp guard policy, on page 65
- show ipv6 dhcp-ldra, on page 67
- show ipv6 dhcp pool, on page 70
- show ipv6 dhcp interface, on page 72
- show ipv6 dhcp relay binding, on page 75
- show ipv6 dhcp route, on page 77

- show ip nat pool platform, on page 78
- show ip nat pool name platform, on page 79
- show ipv6 nat statistics, on page 80
- show ipv6 nat translations, on page 81
- show logging ip access-list, on page 83
- show mdns cache, on page 85
- show mdns cache mac, on page 87
- show mdns cache static, on page 89
- show mdns requests, on page 91
- show mdns service-types, on page 93
- show mdns statistics, on page 95
- show nat64, on page 97
- show nat64 adjacency, on page 101
- show nat64 aliases, on page 103
- show nat64 ha status, on page 105
- show nat64 limits, on page 107
- show nat64 map-t, on page 109
- show nat64 mappings dynamic, on page 110
- show nat64 pools, on page 112
- show nat64 prefix stateful, on page 114
- show nat64 prefix stateless, on page 116
- show nat64 routes, on page 118
- show nat64 services, on page 120
- show nat64 statistics, on page 122
- show nat64 timeouts, on page 124
- show nat64 translations, on page 125
- show nat64 translations entry-type, on page 128
- show nat64 translations redundancy, on page 130
- show nat64 translations time, on page 132
- show nat64 translations total, on page 134
- show nat64 translations v4, on page 136
- show nat64 translations v6, on page 138
- show nat64 translations verbose, on page 140
- show nhrp debug-condition, on page 143
- show nhrp group-map, on page 144
- show platform hardware qfp feature, on page 146
- show platform hardware qfp feature alg statistics sip, on page 150
- show platform software trace message, on page 153
- show redundancy application control-interface group, on page 156
- show redundancy application data-interface, on page 157
- show redundancy application faults group, on page 158
- show redundancy application group, on page 159
- show redundancy application if-mgr, on page 163
- show redundancy application protocol, on page 165
- show redundancy application transport, on page 167
- show running-config mdns-sd policy, on page 168

- show running-config mdns-sd service-instance, on page 170
- show running-config mdns-sd service-list, on page 172
- show running-config vrf, on page 174
- show tech nat, on page 177
- sip address, on page 179
- sip domain-name, on page 180
- snmp-server enable traps dhcp, on page 181
- source-interface (mDNS), on page 182
- subnet prefix-length, on page 184
- term ip netmask-format, on page 187
- timers hellotime, on page 188
- trusted-port (DHCPv6 Guard), on page 190
- update arp, on page 191
- update dns, on page 193
- utilization mark high, on page 195
- utilization mark low, on page 197
- view (DNS), on page 198
- vrf (DHCP pool), on page 201
- vrf (DHCPv6 pool), on page 202

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.

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 limits all-host

To display the current Network Address Translation (NAT) limit entries of all configured hosts, use the **show ip nat limits all-host** command in user EXEC or privileged EXEC mode.

show ip nat limits all-host [**host-address** *host-address* [*end-host-address*] | **number-of-sessions** {**greater-than** | **less-than**} *number*] [**total**]

Syntax Description

host-address	(Optional) Displays statistics for a given address or range of addresses.
host-address	Address of the host or the starting address in a range.
end-host-address	(Optional) Ending address in a range.
number-of-sessions	(Optional) Displays statistics for limit entries with the given number of sessions.
greater-than	(Optional) Displays statistics for limit entries with more than the given number of sessions.
less-than	(Optional) Displays statistics for limit entries with less than the given number of sessions.
number	(Optional) Number of sessions for comparison. The range is from 0 to 2147483647.
total	(Optional) Displays only the total number of entries for a given query.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You can use the **ip nat translation max-entries all-host** command to limit the all-host NAT entries.

When you specify the **total** keyword with the **show ip nat limits all-host** command, the output displays only the total entries for a given query.

Examples

The following is sample output from the **show ip nat limits all-host** command:

```
Router# show ip nat limits all-host

Host            Max Entries  Use Count   Miss Count
------------------------------------------------

10.1.1.2         100000       1           0

Total number of limit entries: 1
```

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

Table 1: show ip nat limits all-host Field Descriptions

Field	Description
Host	The inside local or the outside global IP address of the host. The host is the inside local IP address for inside source translations and the outside global IP address for outside source translations.
Max Entries	The configured maximum number of limit entries.
Use Count	The current number of translations for the limit entry.
Miss Count	Number of times a translation entry was not created because of the use count exceeding the configured maximum for the limit entry.

Related Commands

Command	Description
ip nat translation max-entries	Limits the number of NAT translations to a specified maximum.
show ip nat statistics	Displays NAT statistics

show ip nat limits all-vrf

To display the current Network Address Translation (NAT) limit entries for all configured VPN routing and forwarding (VRF) instances, use the **show ip nat limits all-vrf** command in user EXEC or privileged EXEC mode.

show ip nat limits all-vrf [**vrf-name** *name* | **number-of-sessions** {**greater-than** | **less-than**} *number*] [**total**]

Syntax Description

vrf-name	(Optional) Displays statistics for a specified VRF.
name	VRF name.
number-of-sessions	(Optional) Displays statistics for limit entries with the given number of sessions.
greater-than	(Optional) Displays statistics for limit entries with more than the given number of sessions.
less-than	(Optional) Displays statistics for limit entries with less than the given number of sessions.
number	(Optional) Number of sessions for comparison. The range is from 0 to 2147483647.
total	(Optional) Displays only the total number of entries for a given query.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You can use the **ip nat translation all-vrf** command to limit the all-VRF NAT entries.

When you specify the **total** keyword with the **show ip nat limits all-vrf** command, the output displays only the total entries for a given query.

Examples

The following is sample output from the **show ip nat limits all-vrf** command:

```
Router# show ip nat limits all-vrf

VRF Name        Max Entries  Use Count   Miss Count
-------------------------------------------------

VRF1             100000       1           0

Total number of limit entries: 1
```

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

Table 2: show ip nat limits all-vrf Field Descriptions

Field	Description
VRF Name	Name of the VRF instance.
Max Entries	The configured maximum number of limit entries.
Use Count	The current number of translations for the limit entry.
Miss Count	Number of times a translation entry was not created because of the use count exceeding the configured maximum for the limit entry.

Related Commands

Command	Description
ip nat translation max-entries	Limits the number of NAT translations to a specified maximum.
show ip nat statistics	Displays NAT statistics

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.

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 3: 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.
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.

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 4: show ip nat nvi translations Field Descriptions

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

Field	Description
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 redundancy

To display the Network Address Translation (NAT) high-availability information, use the **show ip nat redundancy** command in privileged EXEC mode.

show ip nat redundancy *rg-id*

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **show ip nat redundancy** command to display information about the NAT high-availability Finite State Machine (FSM) and RG statistics.

The following is sample output from the **show ip nat redundancy** command. The output fields are self-explanatory.

```
Device1# show ip nat redundancy 1

        RG ID: 1        RG Name: RG1
        Current State: IPNAT_HA_RG_ST_ACT_BULK_DONE
        Previous State: IPNAT_HA_RG_ST_ACTIVE
        Recent Events: Curr: IPNAT_HA_RG_EVT_RF_ACT_STBY_HOT
                       Prev: IPNAT_HA_RG_EVT_RF_ACT_STBY_BULK_START

        Statistics :
                Static Mappings: 1,     Dynamic Mappings: 0
                Sync-ed Entries :
                        NAT Entries: 0, Door Entries: 0
                Mapping ID Mismatches: 0
                Forwarded Packets: 0,   Dropped Packets : 0
                Redirected Packets: 0


Device2# show ip nat redundancy 1

        RG ID: 1        RG Name: RG1
        Current State: IPNAT_HA_RG_ST_STBY_HOT
        Previous State: IPNAT_HA_RG_ST_STBY_COLD
        Recent Events: Curr: IPNAT_HA_RG_EVT_RF_STBY_COLD
                       Prev: IPNAT_HA_RG_EVT_NAT_CFG_REF

        Statistics :
                Static Mappings: 1,     Dynamic Mappings: 0
                Sync-ed Entries :
                        NAT Entries: 0, Door Entries: 0
                Mapping ID Mismatches: 0
                Forwarded Packets: 0,   Dropped Packets : 0
```

```
                                Redirected Packets: 0
```

Related Commands

Command	Description
show ip nat translations redundancy	Displays active NAT translations.

show ip nat statistics

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

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged 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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The NAT limit statistics for all hosts and for all VPN routing and forwarding (VRF) instances were removed from the output of this 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 5: 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 created and is decremented each time a translation is cleared or times out.

Field	Description
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	Indicates that 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.
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 statistics platform

The **show ip nat statistics platform** command, displays combined results of the following commands:

- **show platform hardware qfp active feature nat datapath stats**
- **show platform software nat fp active qfp-stats**
- **show platfor software Nat fp active msg-stats**
- **show platform hardware qfp active feature nat datapath esp**
- **show platform hardware qfp active feature nat datapath door**

show ip nat statistics platform

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

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

Examples

```
Device# show ip nat statistics platform

non_extended 0 entry_timeouts 0 statics 0 static net 0 hits 1752915 flowdb_hits 0 misses 0
non_natted_in2out 0 nat_bypass 0 non_natted_out2in 17805
Proxy stats:
ipc_retry_fail 0 cfg_rcvd 2 cfg_rsp 2
Number of sess 10 udp 10 tcp 0 icmp 0
Dump NAT QFP client stats
interface add: 6, upd: 0, del: 0, ack: 6, err: 0
timeout set: 12, ack: 12, err: 0
service set: 28, ack: 28, err: 0
modify-in-progress set: 0, ack: 0, err: 0
esp set: 0, ack: 0, err: 0
dnsv6 set: 1, ack: 1, err: 0
settings set: 0, ack: 0, err: 0
PAP settings set: 0, ack: 0, err: 0
Flow entries set: 1, ack: 1, err: 0
pool add: 1, del: 0, ack: 1, err: 0
addr range add: 1, upd: 0, del: 0, ack: 1, err: 0
static mapping add: 0, upd: 0, del: 0, ack: 0, err: 0
dyn mapping add: 1, upd: 0, del: 0, ack: 1, err: 0
dyn pat mapping add: 0, del: 0, ack: 0, err: 0
porlist add: 0, del: 0, ack: 0, err: 0
```

```
Logging add: 0, upd: 0, del: 0, ack: 0, err: 0
Per-VRF logging add: 0, upd: 0, del: 0, ack: 0, err: 0
Sess replicate add: 0, upd: 0, del: 0, ack: 0, err: 0
max entry set: 1, clr: 0, ack: 1, err: 0
ifaddr change notify: 0, ack: 0, err: 0
debug set: 0, clr: 0, ack: 0, err: 0
dp static-rt add: 0, del: 0, err: 0
dp ipalias add: 1, del: 0, err: 0
dp portlist req: 0, ret: 0, err: 0
dp wlan sess est: 0, term: 0, err: 0
mib setup enable: 0, disable: 0, ack: 0, err: 0
mib addr-bind query: 0, reply: 0, err: 0
MISC settings set: 0, ack: 0, err: 0
Gatekeeper settings set: 0, ack: 0, err: 0
Dump NAT RP-FP message stats
interface cfg: 4, add: 4, del: 0, upd: 0
timeout cfg: 12, add: 12, del: 0
service cfg: 28, add: 28, del: 0, upd: 0
modify-in-progress cfg: 0, add: 0, del: 0, upd: 0
esp cfg: 0, add: 0, del: 0, upd: 0
dnsv6 cfg: 1, add: 1, del: 0, upd: 0
settings cfg: 0, add: 0, del: 0, upd: 0
PAP settings cfg: 0, add: 0, del: 0, upd: 0
non-CLI clear translations exec: 0
pool cfg: 1, add: 1, del: 0, upd: 0
addr range cfg: 1, add: 1, upd: 0, del: 0
static mapping cfg: 0, add: 0, del: 0, upd: 0
dyn mapping cfg: 1, add: 1, del: 0, upd: 0
porlist event: 0, add: 0, del: 0
logging cfg: 0, add: 0, del: 0, upd: 0
per-VRF logging cfg: 0, add: 0, del: 0, upd: 0
replicate cfg: 0, add: 0, del: 0, upd: 0
max entry cfg: 0, add: 0, del: 0, upd: 0
Flow entries cfg: 1, add: 0, del: 0, upd: 0
ifaddr change event: 0
MIB query: 0
MISC settings cfg: 0
Gatekeeper settings cfg: 0, add: 0, del: 0, upd: 0
dp static-rt add: 0, del: 0
dp ipalias add: 1, del: 0
dp portlist req: 0, ret: 0
Stale event start: 0, end: 0
static translation cfg: 0, add: 0, del: 0, upd: 0
ESP global stats: esp_count 0 esp_limit_fail_count 0
DOOR global stats: door_count 0
```

show ip nat translations

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

show ip nat translations [**inside** *global-ip*] [**outside** *local-ip*] [**esp**] [**icmp**] [**pptp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name* [**interface** *interface-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.
interface	(Optional) Displays NAT translations where the session's interface matches the specified output interface.
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.
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.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was modified. The output of this command was updated to display details about NAT port parity and conservation.
26.1.1	The **interface** keyword was added.

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

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

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

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

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

Table 6: 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.

Field	Description
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended--Extended translation • static--Static translation • destination--Rotary translation • outside--Outside translation • timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Related Commands

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

show ip nat translation entry-id platform

To display results of **show platform hardware qfp active feature nat datapath sess-key** command, use the **show ip nat translation entry-id platform** command in user EXEC or privileged EXEC mode.

show ip nat translation entry-idplatform

Syntax Description

entry-id	The hexadecimal value that can ne retrieved from the **show ip nat translation verbose** command. For example: `show ip nat translations verbose` `Pro Inside global Inside local Outside local Outside global` `udp 59.59.1.1:1024 5.0.0.2:1024 6.0.0.2:63 6.0.0.2:63` `create: 02/28/18 05:57:47, use: 02/28/18 20:55:46, timeout: 00:05:00` `Map-Id(In): 1` `Flags: unknown` `Appl type: none` `WLAN-Flags: unknown` `Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet0/0/0` **`entry-id: 0xe8f7e230.`**

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show ip nat translation entry-id platform** command :

Examples

```
Device# show ip nat translation entry-id 0xe8f7e230 platform

ioaddr 5.0.0.2 ooaddr 6.0.0.2 ioport 1024 ooport 63 vrf 0 proto 17 limit type 1
itaddr 59.59.1.1 otaddr 6.0.0.2 itport 1024 otport 63 tableid 0
inmap 0xe9e455c0 outmap 0x0 nak_retry 0inmapid 1
inbindpar 0x0 outbindpar 0x0
insesspar 0x0 outsesspar 0x0
ipsec cookie or spi 0x0 timeout 300 last use ts 0xd2d9 0
appl data 0x0 flags 0x0 ifhandle 8 appl_type 43 rg 0
create time 26 refcnt 1
```

show ip nat translations redundancy

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

show ip nat translations redundancy *rg-id* [**verbose**]

Syntax Description

rg-id	Redundancy group (RG) ID. Valid values are 1 and 2.
verbose	(Optional) Displays additional information for each translation table entry, including the time period when the entry was created and the duration for which it was used.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **show ip nat translations redundancy** command to display information about the NAT translations that belong to a specified RG.

Examples

The following is sample output from the **show ip nat translations redundancy** command for RG ID 1. The output fields are self-explanatory.

```
Device# show ip nat translations redundancy 1 verbose
--- 10.1.1.2            192.0.2.3            ---                ---
    create 00:00:10, use 00:00:10 timeout:0,
    flags:
static, created-by-local, use_count: 0, router/rg id: 0/1 ha_entry_num: 0 mapp_id[in/out]:
 120/0, entry-id: 1, lc_entries: 0
```

Related Commands

Command	Description
show ip nat redundancy	Displays NAT redundancy information.

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**] [**remote**] [**local**]

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.
remote	Displays the NHRP cache entries for remote networks. **Note** By default, cache entries for both local and remote networks are displayed.
local	Displays the NHRP cache entries for local networks. **Note** By default, cache entries for both local and remote networks are displayed.
self	(Optional) Displays the NHRP fake cache information
summary	(Optional) Displays the summary of NHRP cache

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.
Cisco IOS XE Release 17.7.1.a	The **remote** and **local** keywords were integrated in this release.

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 7: 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
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel

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

Examples

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

```
Router# show ip nhrp local
Load for five secs: 100%/36%; one minute: 99%; five minutes: 99%
```

```
No time source, *12:44:19.808 UTC Tue Dec 7 2021

192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:08, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
    (no-socket)
```

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

```
Router# show ip nhrp local detail
Load for five secs: 100%/48%; one minute: 99%; five minutes: 99%
No time source, *12:44:52.971 UTC Tue Dec 7 2021

192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:41, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
   Preference: 255
    (no-socket)
```

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

```
Router# show ip nhrp local dynamic
Load for five secs: 99%/29%; one minute: 99%; five minutes: 99%
No time source, *12:45:15.567 UTC Tue Dec 7 2021
```

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

```
Router# show ip nhrp remote
Load for five secs: 99%/16%; one minute: 99%; five minutes: 99%
No time source, *12:45:36.789 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:41, expire 00:12:55
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:30, expire 00:12:36
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:01, expire 00:14:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:08, expire 00:12:51
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:19, expire 00:07:41
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:07:27, expire 00:14:57
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:08:30, expire 00:06:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:22, expire 00:12:34
```

```
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:05, expire 00:11:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:41, expire 00:06:29
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:07, expire 00:07:52
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:01, expire 00:14:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:14:01, expire 00:00:58
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:00:56, expire 00:14:03
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.15.1
10.1.0.16/32 via 10.1.0.16
   Tunnel0 created 00:13:01, expire 00:11:07
```

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

```
Router# show ip nhrp remote detail
Load for five secs: 99%/27%; one minute: 99%; five minutes: 99%
No time source, *12:45:49.796 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:54, expire 00:12:42
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
   Preference: 192
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:43, expire 00:12:23
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
   Preference: 192
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:14, expire 00:14:18
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
   Preference: 192
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:21, expire 00:12:38
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
   Preference: 192
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:32, expire 00:07:28
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
   Preference: 192
10.1.0.7/32 via 10.1.0.7
  Tunnel0 created 00:07:40, expire 00:14:44
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
```

```
   Preference: 192
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:08:43, expire 00:14:47
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
   Preference: 192
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:35, expire 00:12:21
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
   Preference: 192
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:18, expire 00:11:01
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
   Preference: 192
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:54, expire 00:06:16
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
   Preference: 192
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:20, expire 00:07:39
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
   Preference: 192
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:14, expire 00:14:01
   Type: dynamic, Flags: registered nhop bfd
```

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

```
Router# show ip nhrp remote dynamic
Load for five secs: 100%/12%; one minute: 99%; five minutes: 99%
No time source, *12:48:52.151 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:11:56, expire 00:12:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.2/32 via 10.1.0.2
   Tunnel0 created 00:02:46, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.2.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:20:45, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:05:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:10:34, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:10:42, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
```

```
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:11:45, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:09:38, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:16:20, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:15:56, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:10:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:17:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:04:11, expire 00:12:32
```

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

```
Router# show ip nhrp remote dynamic
Load for five secs: 55%/3%; one minute: 62%; five minutes: 87%
No time source, *12:50:24.793 UTC Tue Dec 7 2021

10.0.0.1/32 via 10.0.0.1
   Tunnel0 created 06:46:47, never expire
   Type: static, Flags: router unique local
   NBMA address: 1.1.1.1
    (no-socket)
Metadata Exchange Framework:
Type State
1   Reset
MEF ext data:0x0
2   Reset
MEF ext data:0x0
3   Reset
MEF ext data:0x0
```

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

```
Router# show ip nhrp remote summary
Load for five secs: 20%/0%; one minute: 50%; five minutes: 79%
No time source, *12:51:38.026 UTC Tue Dec 7 2021

IP NHRP cache 10000 entries, 7680000 bytes
    1 static   9999 dynamic    0 incomplete
9999 Remote
    0 static   9999 dynamic    0 incomplete
    9999 nhop     9999 bfd
    0 default  0 temporary
```

```
    0 route
        0 rib (0 H    0 nho)
        0 bgp
    0 lfib
1 Local
    1 static   0 dynamic    0 incomplete
    0 lfib
```

The following is sample output from the **show ip nhrp remote static tu1** command:

```
Router# show ip nhrp remote static tu1
10.0.0.1/32 (VPN1) via 10.0.0.1
   Tunnel1 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
spoke1#sh ip nhrp remote static tu11
10.0.0.1/32 (VPN11) via 10.0.0.1
   Tunnel11 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
```

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

Table 8: 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.

Field	Description
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 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 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).

Field	Description
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 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.
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.

Command	Description
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.

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 9: 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-addressinterface*]

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 10: Interface Types, Valid Numbers, and Interface Descriptions

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

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

Examples

The following is sample output from the **show ip nhrp 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 11: 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. • 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.

Command	Description
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip nhrp multicast stats

To display multicast mapping statistics for one or all interfaces, use the **show ip nhrp multicast stats** command in privileged EXEC mode. The command displays statistics such as the count of enqueued, dequeued, and dropped packets.

show ip nhrp multicast [*interface-name*] **stats**

Syntax Description

interface-name	Displays multicast mapping statistics for the specified interface. Example: **show ip nhrp multicast tunnel0 stats**

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.8.1	Command introduced.

Example

```
Router#show ip nhrp multicast stats
Legend: (m/n) - (m packets/n milliseconds)
================================================================================================

Global stats
Total multicast pkts enqueued    102
Total multicast failed to enqueue 0
Total multicast pkts dequeued     102
Invalid multicast pkts dequeued   0
Total multicast pkts dropped      0

Interface stats
                                    Enqueued/Failed             Dequeued/Rep fail       Dropped
                                ------------------------  --------------------------  ----------
 Tu0     (250    /     10)              51/0                         51/0                  0
```

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 12: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ip nhrp nhs detail
Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
  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 13: 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.

Command	Description
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip nhrp redirect

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

show ip nhrp redirect *statistics*

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2SX	This command was introduced.

Examples

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

```
Router# show ip nhrp redirect

I/F      NBMA address          Destination           Drop Count    Expiry

Tunnel43   10.232.195.197         10.138.140.33          2     00:00:05
Tunnel43   10.232.195.193         10.138.140.33         54     00:00:05
Tunnel43   10.232.195.185         10.138.140.33          1     00:00:06
Tunnel43   10.232.195.189         10.138.140.33          0     00:00:07
Tunnel43   10.232.195.205         10.138.153.66         52     00:00:07
```

This output shows the content of the NHRP redirect table on the node. An entry in output indicates that further redirect messages to the NBMA address for the destination will be suppressed as long as the corresponding entry doesn't expire

The table below describes the fields shown in the command output.

Table 14: show ip nhrp redirect command- Field Descriptions

Field Output	Description
NBMA Address	Displays the address where the redirect message is sent to. This is the NBMA address of the source spoke.
Destination	Displays the destination IP address from the data packet that triggered the NHRP redirect. This is the LAN address that is behind the destination spoke.
Drop Count	Displays the number of redirect messages throttled due to presence of this entry in the redirect table .
Expiry	Displays the lifetime of the redirect entry. The default max lifetime is 8 seconds. At expiry of the lifetime, the entry is deleted and new redirect messages with these details can be sent by this node if there are further data packets matching these entries .

Examples

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

```
Router# show ip nhrp redirect statistics

DMVPN Redirect Indications throttled: 7
```

show ip nhrp summary

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

show ip nhrp summary

Command Modes

User EXEC Privileged EXEC

Command History

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

Examples

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

```
Router# show ip nhrp summary
IP NHRP cache 1 entry, 256 bytes
    1 static  0 dynamic  0 incomplete
```

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

Table 15: 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[**throttled** | **interface** {**tunnel** *number* | **Virtual-Access** *number*}]

Syntax Description

throttled	(Optional) Displays information about NHRP traffic that is throttled.
interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	Specifies the tunnel interface number.
Virtual-Access *number*	Specifies the virtual access interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.4(6)T	This command was modified. The show output was enhanced to display information about traffic indication (redirects).
12.4(9)T	This command was modified. 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 integrated into Cisco IOS XE Release 2.5.
15.3(2)T	This command was modified. The **Virtual-Access** *number* keyword-argument pair was added.
Cisco IOS XE 16.3.2	This command was modified. The **throttled** keyword was added.

Usage Guidelines

Replacing **ip** in the command name with **ipv6** shows IPv6-specific traffic.

Examples

The following example shows sample output for NHRP traffic statistics for tunnel interface 0:

```
Device# 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 16: 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.

The following example shows sample output for the **show ip nhrp traffic** command with the **throttled** keyword applied:

```
SPOKE1#show ip nhrp traffic throttled
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

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.

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.

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.

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 17: 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.

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 ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The **show ipv6 dhcp** command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples

The following is sample output from the **show ipv6 dhcp**command. The output is self-explanatory:

```
Router# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4	This command was modified. Command output was updated to display a PPP username associated with a binding.
12.4(24)T	This command was modified. Command output was updated to display address bindings.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name*keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
```

```
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

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

Table 18: show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username is associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as "unassigned."

The following example shows that the PPP username associated with the binding is "client_1":

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
```

```
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

The following example shows that the PPP username associated with the binding is unassigned:

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

Syntax Description

agent-URL	(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the **ipv6 dhcp database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show ipv6 dhcp database**command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Examples

The following is sample output from the **show ipv6 dhcp database**command:

```
Router# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
```

```
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

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

Table 19: show ipv6 dhcp database Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before terminating a database transfer. Transfers that exceed the timeout period are terminated.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires.
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
ipv6 dhcp database	Specifies DHCP for IPv6 binding database agent parameters.

show ipv6 dhcp guard policy

To display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard information, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

show ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

If the *policy-name* argument is specified, only the specified policy information is displayed. If the *policy-name* argument is not specified, information is displayed for all policies.

Examples

The following is sample output from the **show ipv6 dhcp guard guard** command:

```
Router#show ipv6 dhcp guard policy

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Et0/3

Dhcp guard policy: test1
        Device Role: dhcp server
        Target: vlan 0    vlan 1    vlan 2    vlan 3    vlan 4
        Max Preference: 200
        Min Preference: 0
        Source Address Match Access List: acl1
        Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
        Device Role: dhcp relay
        Target: Et0/0 Et0/1 Et0/2
```

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

Table 20: show ipv6 dhcp guard Field Descriptions

Field	Description
Device Role	The role of the device. The role is either client, server or relay.

Field	Description
Target	The name of the target. The target is either an interface or a VLAN.

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

show ipv6 dhcp-ldra

To display configuration details and statistics for a Lightweight DHCPv6 Relay Agent (LDRA), use the **show ipv6 dhcp-ldra** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp-ldra [statistics]

Syntax Description

statistics	(Optional) Displays LDRA-related statistics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to view the number and type of DHCPv6 packets received or processed, the number and type of DHCPv6 messages dropped, error counters, and the interface state (client-facing trusted interface, server-facing interface, and so on).

You can also view LDRA configuration details, such as the type of LDRA configuration and the interface or VLAN where the LDRA is configured.

Example

The following sample output displays LDRA configuration details before initiating a DHCP session. The fields in the example below are self-explanatory.

```
Device> enable
Device # show ipv6 dhcp-ldra statistics


             DHCPv6 LDRA client facing statistics.

Messages received               0
Messages sent                   0
Messages discarded              0

                DHCPv6 LDRA server facing statistics.

Messages received               0
Messages sent                   0
Messages discarded              0
```

The following sample output displays LDRA configuration details after initiating a DHCP session. The fields in the example below are self-explanatory.

```
Device> enable

Device # show ipv6 dhcp-ldra statistics


               DHCPv6 LDRA client facing statistics.

Messages received               2
Messages sent                   2
Messages discarded              0

Messages                        Received
SOLICIT                         1
REQUEST                         1

Messages                        Sent
RELAY-FORWARD                   2

                DHCPv6 LDRA server facing statistics.


Messages received               2
Messages sent                   2
Messages discarded              0

Messages                        Received
RELAY-REPLY                     2

Messages                        Sent
ADVERTISE                       1
REPLY                           1
```

The following sample output displays LDRA configuration details. The fields in the example below are self-explanatory.

```
Device> enable
Device # show ipv6 dhcp-ldra



DHCPv6 LDRA is Enabled.
DHCPv6 LDRA policy: client-facing-disable
       Target: none
DHCPv6 LDRA policy: client-facing-trusted
       Target: vlan 5
DHCPv6 LDRA policy: client-facing-untrusted
       Target: none
DHCPv6 LDRA policy: server-facing
       Target: Gi1/0/7
```

Related Commands

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

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp pool [*poolname*]

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	Command output was updated to display address pools and prefix pools.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a configuration pool, and use the **ipv6 dhcp server** command to associate the configuration pool with a server on an interface.

The **show ipv6 dhcp pool** command displays DHCP for IPv6 configuration pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, information about all pools is shown.

Examples

The following sample output displays DHCP for IPv6 configuration pool information:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
```

```
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
```

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

Table 21: show ipv6 dhcp pool Field Descriptions

Field	Description
DHCPv6 pool: svr-p1	The name of the pool.
IA PD	Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes to be delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	Lifetimes, in seconds, associated with the prefix statically assigned to the specified client.
DNS server	IPv6 addresses of the DNS servers.
Domain name	Displays the DNS domain search list.
Active clients	Total number of active clients.

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	Command output was modified to allow relay agent information to be displayed on a specified interface if the relay agent feature is configured on that interface.
12.4(24)T	Command output was updated to display interface address assignments and T1 and T2 renew/rebind times.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface**command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
```

```
    Prefix: 3FFE:C00:C18:1::/72
            preferred lifetime 240, valid lifetime 54321
            expires at Nov 08 2002 09:10 AM (54319 seconds)
    Prefix: 3FFE:C00:C18:2::/72
            preferred lifetime 300, valid lifetime 54333
            expires at Nov 08 2002 09:11 AM (54331 seconds)
    Prefix: 3FFE:C00:C18:3::/72
            preferred lifetime 280, valid lifetime 51111
            expires at Nov 08 2002 08:17 AM (51109 seconds)
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: domain1.net
  Domain name: domain2.net
  Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled
```

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

Table 22: show ipv6 dhcp interface Field Descriptions

Field	Description
Ethernet2/1 is in server/client mode	Displays whether the specified interface is in server or client mode.
Preference value:	The advertised (or default of 0) preference value for the indicated server.
Prefix name is cli-p1	Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.
Using pool: svr-p1	The name of the pool that is being used by the interface.
State is OPEN	State of the DHCP for IPv6 client on this interface. "Open" indicates that configuration information has been received.
List of known servers	Lists the servers on the interface.
Address, DUID	Address and DHCP unique identifier (DUID) of a server heard on the specified interface.
Rapid commit is disabled	Displays whether the **rapid-commit** keyword has been enabled on the interface.

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the **show ipv6 dhcp interface** command displays relay agent information on FastEthernet interface 0/0:

```
Router(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Router# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
  Relay destinations:
    FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

Related Commands

Command	Description
ipv6 dhcp client pd	Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.

Command	Description
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp relay binding

To display DHCPv6 Internet Assigned Numbers Authority (IANA) and DHCPv6 Identity Association for Prefix Delegation (IAPD) bindings on a relay agent, use the **show ipv6 dhcp relay binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp relay binding [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
Cisco IOS XE Release 3.5S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
12.2(33)SCF4	This command was implemented on Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

If the **vrf** *vrf-name* keyword-argument pair is specified, all bindings belonging to the specified VRF are displayed.

Note Only the DHCPv6 IAPD bindings on a relay agent are displayed on the Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.

Examples

The following is sample output from the **show ipv6 dhcp relay binding** command:

```
Device# show ipv6 dhcp relay binding
```

The following example shows output from the **show ipv6 dhcp relay binding** command with a specified VRF name on a Cisco uBR10012 universal broadband device:

```
Device# show ipv6 dhcp relay binding vrf vrf1

Prefix: 2001:DB8:0:1:/64 (Bundle100.600)
  DUID: 000300010023BED94D31
```

```
IAID: 3201912114
lifetime: 600
```

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

Table 23: show ipv6 dhcp relay binding Field Descriptions

Field	Description
Prefix	IPv6 prefix for DHCP.
DUID	DHCP Unique Identifier (DUID) for the IPv6 relay binding.
IAID	Identity Association Identification (IAID) for DHCP.
lifetime	Lifetime of the prefix, in seconds.

Related Commands

Command	Description
clear ipv6 dhcp relay binding	Clears a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding.

show ipv6 dhcp route

To display routes added by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) on the DHCPv6 server for Internet Assigned Numbers Authority (IANA) and Identity Association for Prefix Delegation (IAPD), use the **show ipv6 dhcp route** command in privileged EXEC mode.

show ipv6 dhcp route {**vrf** *vrf-name*} {**ipv6-addressipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Displays all the DHCPv6 relay bindings.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show ipv6 dhcp route** command:

```
Router# show ipv6 dhcp route vrf vrfname 2001:0DB8:3333:4::5/126
```

Related Commands

Command	Description
ipv6 dhcp iana-route-add	Adds routes for individually assigned IPv6 addresses on a relay or server.
ipv6 dhcp iapd-route-add	Enables route addition by the DHCPv6 relay and server for the delegated prefix.

show ip nat pool platform

To display results of **show platform software nat fp active pool** command, use the **show ip nat pool platform** command in user EXEC or privileged EXEC mode.

show ip nat pool platform

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

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

Examples

```
Device# show ip nat pool name natpool1 platform

Dump NAT pool config
ID: 1, Name: nat_pool1, Type: Generic, Mask: 255.255.0.0
Flags: Unknown, Acct name:
Address range blocks: 1
Start: 192.0.2.1, End: 192.0.2.254
Last stats update: 02/28 05:57:02.263
Last refcount value: 1
```

show ip nat pool name platform

To display combined results of **show platform hardware qfp active feature nat datapath pool** and **show platform software nat f0 pool-stats id** command, use the **show ip nat pool name platform** command in user EXEC or privileged EXEC mode.

show ip nat pool platform

Syntax Description

pool-name	Name of the NAT address pool for which information will be displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show ip nat pool name platform** command :

Examples

```
Device# show ip nat pool name natpool1 platform

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
```

show ipv6 nat statistics

To display Network Address Translation--Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics**command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show ipv6 nat statistics**command:

```
Router# show ipv6 nat statistics
Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1  Misses: 1
Expired translations: 0
```

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

Table 24: show ipv6 nat statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation.
NAT-PT interfaces	The interfaces, by type and number, that are configured to run NAT-PT translations.
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.

Related Commands

Command	Description
show ipv6 nat translations	Displays active NAT-PT translations.

show ipv6 nat translations

To display active Network Address Translation--Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [**icmp** | **tcp** | **udp**] [**verbose**]

Syntax Description

icmp	(Optional) Displays detailed information about NAT-PT ICMP translation events.
tcp	(Optional) Displays detailed information about NAT-PT TCP translation events.
udp	(Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
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
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

```
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,52922      2001::2,52922
---   192.168.124.8            3002::8
      192.168.123.2            2001::2
---   192.168.124.8            3002::8
      ---                      ---
---   192.168.121.4            5001::4
      ---                      ---
```

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

```
Router# show ipv6 nat translations verbose
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
```

```
---   ---                       ---
      192.168.123.2             2001::2
      create 00:04:24, use 00:03:24,
---   ---                       ---
      192.168.122.10            2001::10
      create 00:04:24, use 00:04:24,
tcp   192.168.124.8,11047       3002::8,11047
      192.168.123.2,23          2001::2,23
      create 00:03:24, use 00:03:20, left 00:16:39,
udp   192.168.124.8,52922       3002::8,52922
      192.168.123.2,69          2001::2,69
      create 00:02:51, use 00:02:37, left 00:17:22,
udp   192.168.124.8,52922       3002::8,52922
      192.168.123.2,52922       2001::2,52922
      create 00:02:48, use 00:02:30, left 00:17:29,
---   192.168.124.8             3002::8
      192.168.123.2             2001::2
      create 00:03:24, use 00:02:34, left 00:17:25,
---   192.168.124.8             3002::8
      ---                       ---
      create 00:04:24, use 00:03:24,
---   192.168.121.4             5001::4
      ---                       ---
      create 00:04:25, use 00:04:25,
```

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

Table 25: show ipv6 nat translations Field Descriptions

Field	Description
Prot	Protocol of the port identifying the address.
IPv4 source/IPv6 source	The IPv4 or IPv6 source address to be translated.
IPv4 destination/IPv6 destination	The IPv4 or IPv6 destination address.
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).
left	Time before the entry times out (in hours:minutes:seconds).

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.

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.

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

show mdns cache

To display multicast Domain Name System (mDNS) cache information, use the **show mdns cache** command in user EXEC or privileged EXEC mode.

show mdns cache [**interface** *type number* [**detail**] | [**name** *record-name*] [**type** *record-type*] [**detail**]]

Syntax Description

interface *type number*	(Optional) Displays mDNS cache information for the specified interface.
detail	(Optional) Displays detailed mDNS cache information for the specified interface or record. **Note** You can use the **detail** keyword for a specific interface, record or type. You cannot use it independently with the **show mdns cache** command.
name *record-name*	(Optional) Displays mDNS cache information for the specified record.
type *record-type*	(Optional) Displays mDNS cache information for the specific record type.

Note You can view mDNS cache information for a specific record type and record name by using the keyword-argument pair combination **name** *record-name* **type** *record-type*.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Examples

The following sample output displays mDNS cache information :

```
Device> enable
Device# show mdns cache


mDNS CACHE
==================================
 [<NAME>] [<TYPE>][<CLASS>] [<TTL>/Remaining] [Accessed] [If-index] [<RR
 Record Data>]
```

```
_services._dns-sd._udp.local PTR IN 4500/4496 0 3 _ipp._tcp.local

_ipp._tcp.local PTR IN 4500/4496 1 3 printer1._ipp._tcp.local

printer1._ipp._tcp.local TXT IN 4500/4496 1 3 (1)''
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns requests	Displays mDNS request information.
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns cache mac

To display multicast Domain Name System (mDNS) cache information for a specific MAC address, use the **show mdns cache mac** command in user EXEC or privileged EXEC mode.

show mdns cache mac *mac-address* [**detail**]

Syntax Description

mac-address	Displays mDNS cache information for the specified MAC address.
detail	(Optional) Displays detailed mDNS cache information for the specified MAC address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns cache mac** command:

```
Device> enable
Device# show mdns cache mac aabb.cc01.2c10

mDNS CACHE
==================================

[<NAME>]                                                [<TYPE>][<CLASS>]
[<TTL>/Remaining] [Accessed] [If-name] [Mac Address] [<RR Record Data>]
_mdnsgateway._udp.local                                    PTR     IN
1200/1200         1          0
mdnsgateway-Et0/1._mdnsgateway._udp.local
```

The table below describes the significant fields in the display.

Table 26: show mdns cache mac Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TYPE>]	Service type.
[<CLASS>]	DNS class. IN refers to the internet class resource record.

Field	Description
[<TTL>/Remaining]	Time to Live (TTL) value of the service.
[If-name]	Interface name.
[Mac Address]	MAC address of the device.
[<RR Record Data>]	Resource record data. The data includes service instance information and the interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information for the device.
show mdns cache static	Displays mDNS service instance records in cache that are statically registered.

show mdns cache static

To display multicast Domain Name System (mDNS) service instance records in cache that are statically registered, use the **show mdns cache static** command in user EXEC or privileged EXEC mode.

show mdns cache static

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns cache static** command:

```
Device> enable
Device# show mdns cache static

mDNS CACHE
==================================

[<NAME>]                                                [<TYPE>][<CLASS>]
[<TTL>/Remaining] [Accessed] [If-name] [Mac Address] [<RR Record Data>]
_mdnsgateway._udp.local                                    PTR     IN
1200/1200       1       0
mdnsgateway-Et0/1._mdnsgateway._udp.local
_mdnsgateway._udp.local                                    PTR     IN
 600/600        1       0              mdnsgateway._mdnsgateway._udp.local
```

The table below describes the significant fields in the display.

Table 27: show mdns cache static Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TYPE>]	Service type.
[<CLASS>]	DNS class. IN refers to the internet class resource record.
[<TTL>/Remaining]	Time to Live (TTL) value of the service.

Field	Description
[If-name]	Interface name.
[Mac Address]	MAC address of the device.
[<RR Record Data>]	Resource record data. The data includes service instance information and the interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information for the device.
show mdns cache mac	Displays mDNS cache information for a specific MAC address.

show mdns requests

To display multicast Domain Name System (mDNS) request information, use the **show mdns requests** command in privileged EXEC mode.

show mdns requests [**detail** | [**type** *record-type*] [**name** *record-name*]]

Syntax Description

detail	(Optional) Displays detailed mDNS request information, including record name, record type, and record class.
name *record-name*	(Optional) Displays mDNS request information for the specified record.
type *record-type*	(Optional) Displays mDNS request information for a specific record type. **Note** For the *record-type* argument, you must specify one of these record types - PTR, SRV, A, or AAAA.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.13S
15.5(2)S	This command was integrated into Cisco IOS Release 15.5(2)S.

Examples

The following sample output displays detailed mDNS request information :

```
Device> enable
Device# show mdns requests detail


MDNS Outstanding Requests
================================
Request name  :   _ipp._tcp.local
Request type  :   PTR
Request class :   IN
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information.

Command	Description
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns service-types

To display multicast Domain Name System (mDNS) service type information for device interfaces, use the **show mdns service-types** command in user EXEC or privileged EXEC mode.

show mdns service-types [**all** | **interface** *type number*]

Syntax Description

all	(Optional) Displays mDNS service type information for all device interfaces.
interface *type number*	(Optional) Displays mDNS service type information for the specified interface.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Examples

The following is sample output from the **show mdns service-types** command:

```
Device> enable
Device# show mdns service-types


mDNS SERVICES
================================
[<NAME>]            [<TTL>/Remaining] [If-name]

_ipp._tcp.local     4500/4496
```

The table below describes the significant fields in the display.

Table 28: show mdns service-types Field Descriptions

Field	Description
[<NAME>]	Service instance. The service instance is of the specified service type.
[<TTL>/Remaining]	Time to Live (TTL) value of the service.
[If-name]	Interface name.

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns requests	Displays mDNS request information.
show mdns statistics	Displays mDNS statistics for the specified service-list.

show mdns statistics

To display multicast Domain Name System (mDNS) statistics, use the **show mdns statistics** command in user EXEC or privileged EXEC mode.

show mdns statistics {**all** | **interface** *type number* | **service-list** *name* | [**cache** | **service-policy**] {**all** | **interface** *type number*} | **services orderby providers**}

Syntax Description

all	Displays mDNS statistics for the device or service-policy.
interface *type number*	Displays mDNS statistics or service-policy statistics for the specified interface.
service-list *name*	Displays mDNS statistics for the specified service-list.
cache	Displays mDNS cache statistics.
service-policy	Displays mDNS service-policy statistics.
services orderby providers	Displays the number of services learnt from each client. The services are displayed in the descending order; the client from which most number of services are learnt is displayed first on the list, and so on.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.
15.2(2)E	This command was modified. The keyword-argument pair **service-list** *name* and the option to display mDNS statistics for an interface were added. The keywords **cache** and **services orderby providers** were added.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S
15.5(2)S	This command was integrated into Cisco IOS 15.5(2)S Release.

Usage Guidelines

The **all** keyword can be used in two forms of the **show mdns statistics** command. You can view mDNS statistics for the device using the **show mdns statistics all** command form. To view service-policy statistics, use the **show mdns statistics service-policy all** command form.

The keyword-argument pair **interface** *type number* can be used in two forms of the **show mdns statistics** command. To display mDNS statistics for a specific interface, use the **show mdns statistics interface** *type number* command form. To display service-policy statistics for a specific interface, use the **show mdns statistics service-policy interface** *type number* command form.

Examples

The following sample output displays detailed mDNS statistics:

```
Device> enable
Device# show mdns statistics all


 mDNS Statistics
================================
 mDNS packets sent : 0
 mDNS packets received : 31
 mDNS packets dropped : 8
 mDNS cache memory in use: 64264(bytes)
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
show mdns cache	Displays mDNS cache information.
show mdns requests	Displays mDNS request information.

show nat64

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

show nat64 {**logging** | **services** | **timeouts** | **reconciliation** | **replications**}

Syntax Description

logging	Displays NAT64 logging information.
services	Displays NAT64 services information.
timeouts	Displays statistics for a NAT64 translation session timeout.
reconciliation	Displays NAT64 reconciliation information.
replications	Displays NAT64 replication information.

Command Modes

User EXEC (>)

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **reconciliation** and **replications** keywords were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T

Usage Guidelines

NAT64 supports logging of information about all NAT sessions that are created and deleted. All event entries that are logged have a time stamp. Use the output of this command verify your NAT64 configuration.

The output of the **show nat64 reconciliation** command displays information about Forwarding Processor (FP) switchovers. Whenever an FP does a switchover, the Route Processor (RP) and the newly active FP audit their own configuration and alias data to ensure that the RP and the newly active FP are synchronized.

Replication indicates whether the traffic to a port is replicated or not. The **show nat64 replications** command displays the state of any port that needs to be treated specially for replication. By default, HTTP (port 80) sessions are not synchronized.

Examples

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

```
Device# show nat64 logging

NAT64 Logging Type
   Method          Protocol Dst. Address    Dst. Port Src. Port

translation
   flow export     UDP      10.1.1.1         5000      60087
```

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

Table 29: show nat64 logging Field Descriptions

Field	Description
Method	Method used for logging records. Depending on your release, only flow export is supported.
Protocol	Protocol used for translation.
Dst. Address	Destination IPv4 address of the external collector that is configured for logging records.
Dst. Port	Destination port of the external collector that is configured for logging records.
Src. Port	Source port from where logging records are sent out on the network.

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

```
Device# show nat64 services

NAT64 Services

ftp
   UDP Enabled: TRUE
   TCP Enabled: TRUE
   Service Definition
   Protocol: 6 Port: 21
```

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

Table 30: show nat64 services Field Descriptions

Field	Description
UDP Enabled	Indicates whether the service translation is enabled by default for UDP packets if the protocol is supported by the service definition.
TCP Enabled	Indicates whether the service translation is enabled by default for TCP packets if the protocol is supported by the service definition.
Service Definition	Definition of the service (the Protocol and Port fields for which packets are considered a match to the given service).

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

```
Device# show nat64 timeouts
```

```
NAT64 Timeout
   Seconds     CLI Cfg Uses 'All' all flows
   86400       FALSE   FALSE      udp
   300         FALSE   TRUE       tcp
   7200        FALSE   TRUE       tcp-transient
   240         FALSE   FALSE      icmp
   60          FALSE   TRUE
```

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

Table 31: show nat64 timeouts Field Descriptions

Field	Description
Seconds	NAT64 timeout, in seconds.
CLI Cfg	Indicates whether the timeout is explicitly configured through the CLI. The timeout values configured through the CLI change the default timeout values.

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

```
Device# show nat64 reconciliation

 Reconciliation Info

   Start updates received: 0
   End updates received: 0
   Last update received: --- (2)
```

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

Table 32: show nat64 reconciliation Field Descriptions

Field	Description
Start updates received	Indicates the number of synchronization events that are started.
End updates received	Indicates the number of synchronization events that are completed.
Last updated received	Indicates which event was received last—the start or end event.

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

```
Device# show nat64 replications

 Replications configured for http: 1

 NAT64 Replications (ports not shown have replication enabled)
 Traffic Type     Port  Replication User-Configured

 http             80    disable     FALSE
```

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

Table 33: show nat64 reconciliation Field Descriptions

Field	Description
Traffic type	Type of traffic.
Port	Layer 4 port of the traffic.
Replication	Indicates whether the traffic will be replicated or not. Valid values are enable (replicated) or disable (not replicated).
User-Configured	Indicates whether the replication is because of the default behavior (FALSE) of the traffic or user configuration (TRUE).

Related Commands

Command	Description
nat64 logging	Enables NAT64 logging.
nat64 service ftp	Enables NAT64 FTP service.
nat64 translation	Enables NAT64 translation.

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.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

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.

Examples

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

```
Device# 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 34: 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 aliases

To display the IP aliases created by Network Address Translation 64 (NAT64), use the **show nat64 aliases** command in user EXEC or privileged EXEC mode.

show nat64 aliases [**range** *lower-address-range upper-address-range*]

Syntax Description

range	(Optional) Displays information about the IP aliases in a given range.
lower-address-range	(Optional) IPv4 lower address range.
upper-address-range	(Optional) IPv4 upper address range.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

An alias is an address (examples of an address are pool addresses and static mapping addresses) for which the router sends an Address Resolution Protocol (ARP) request even though the address is not configured on an interface. NAT64 maintains a database of all the addresses for which an ARP request is sent. These addresses are inserted in the database as IP aliases when they exist on the subnet of an interface address.

Examples

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

```
Device# show nat64 aliases

Aliases configured: 1

Address   Table ID Inserted  Flags  Send ARP Reconcilable Stale Ref-Count

10.1.1.1    0        FALSE   0x0030 FALSE    TRUE         FALSE 1
```

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

Table 35: show nat64 aliases Field Descriptions

Field	Description
Aliases configured	The number of NAT64 addresses for which an IP alias is configured.
Address	IPv4 address of the alias.

Field	Description
Table ID	VPN routing and forwarding (VRF) table ID that is associated with the alias.
Inserted	Indicates whether the alias is currently inserted as an IP alias.
Send ARP	Indicates whether an ARP request is sent. Valid values are TRUE or FALSE.

Related Commands

Command	Description
nat64 enable	Enables 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.

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 36: show nat64 ha status Field Descriptions

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

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

show nat64 limits

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

The **show nat64 limits** command displays the configured maximum limit for the number of entries that NAT64 translates.

Examples

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

```
Device# show nat64 limits

NAT64 Limit     Max Entries Is Configured

global          200         TRUE
```

The table below describes the fields shown in the display.

Table 37: show nat64 limits Field Descriptions

Field	Description
NAT64 Limit	Indicates whether the NAT64 translation limit is configured globally or on an interface.
Max Entries	The maximum number of entries that NAT64 translates.
Is Configured	Indicates whether the maximum limit is configured. Valid values are True or False.

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

Command	Description
nat64 translation	Enables NAT64 translation.

show nat64 map-t

To display Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) information, use the **show nat64 map-t** command in privileged EXEC mode.

show nat64 map-t [**domain** *number*]

Syntax Description

domain *number*	Displays MAP-T information for a specific domain. Valid values for the *number* argument are from 1 to 128.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

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

Examples

The following is sample output from the **show nat64 map-t domain**command:

```
Device# show nat64 map-t domain 89

MAP-T Domain 89
   Mode MAP-T
   Default-mapping-rule
      Ip-v6-prefix ::/0
   Basic-mapping-rule
      Ip-v6-prefix ::/0
      Ip-v4-prefix 10.1.1.1/32
      Port-parameters
         Share-ratio 34   Contiguous-ports 64   Start-port 3455
         Share-ratio-bits 6   Contiguous-ports-bits 6   Port-offset-bits 4
```

The

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings

show nat64 mappings dynamic

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

show nat64 mappings dynamic [**list** *acl-name* | **pool** *pool-name*]

Syntax Description

list *acl-name*	(Optional) Displays the mappings of a specified access list.
pool *pool-name*	(Optional) Displays the mappings of a specified pool.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Dynamic one-to-one mapping is used to map IPv6 hosts from a pool of available IPv4 addresses on a first-come first-served basis. The dynamic one-to-one configuration is deployed when the number of IPv6 hosts is few and an equal or greater number of public IPv4 addresses are available. For dynamic binds, the mapping is always between an IPv4 address and an IPv6 address.

Examples

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

```
Device# show nat64 mappings dynamic

Dynamic mappings configured: 1

Direction       ACL         Pool        Flags

v6v4            mylist      mypool      0x00000000 (none)
```

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

Table 38: show nat64 mappings dynamic Field Descriptions

Field	Description
Dynamic mappings configured	The number of dynamic mappings configured.
Direction	The direction in which the dynamic mapping is configured.
ACL	Access list name.

Field	Description
Pool	Name of the pool.

Related Commands

Command	Description
nat64 v4v6	Translates an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for NAT64.
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

show nat64 pools

To display the IPv4 address pools for dynamic Network Address Translation 64 (NAT64) mapping, use the **show nat64 pools** command in user EXEC or privileged EXEC mode.

show nat64 pools [**name** *pool-name* | **range** *lower-address-range upper-address-range*] [**routes**]

Syntax Description

name *pool-name*	(Optional) Displays information about the configured address pools listed by the pool name.
range	(Optional) Displays information about address pools within a provided address range.
lower-address-range	(Optional) IPv4 lower address range.
upper-address-range	(Optional) IPv4 upper address range.
routes	(Optional) Displays static routes for a given pool.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Pools allow you to specify an IPv4 address range that is used for dynamic mapping of objects. Only IPv4 address pools and one contiguous address range per pool object is supported in Cisco IOS XE Release 3.4S. When a pool is created, a static route is installed for all addresses in the pool range.

Examples

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

```
Device# show nat64 pools

Pools configured: 1

Protocol Name    Is Single    Range                    Ranges

IPv4     mypool   TRUE        (10.1.1.1 - 10.1.1.10)  10.1.1.1 - 10.1.1.10
```

The table below describes the fields shown in the display.

Table 39: show nat64 pools Field Descriptions

Field	Description
Protocol	Name of the protocol.

Field	Description
Name	Name of the configured pool.
Is Single	Indicates whether the pool contains a single address range or multiple address ranges. The value of the range is displayed. In Cisco IOS XE Release 3.4S only a single address range is supported.
Range	IPv4 address range.
Ranges	All address ranges for the pool. In Cisco IOS XE Release 3.4S only a single address range is supported.

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.
nat64 v4	Enables NAT64 IPv4 configuration.

show nat64 prefix stateful

To display information about Network Address Translation 64 N(AT64) stateful prefixes, use the **show nat64 prefix stateful** command in user EXEC or privileged EXEC mode.

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

Syntax Description

global	Displays information about global prefixes.
interfaces	Displays information about the configured interfaces.
prefix	(Optional) Displays information about interfaces that use a prefix.
ipv6-address	(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.
static-routes	Displays information about prefix static routes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

A maximum of one global stateful prefix and one stateful prefix per interface is supported. NAT64 uses the configured stateful prefix to algorithmically translate the IPv4 addresses of the IPv4 hosts to and from IPv6 addresses. If a global stateful prefix or an interface stateful prefix is not configured, the Well Known Prefix (WKP) of 64:ff9b::/96 is used to translate the IPv4 address of the IPv4 host.

Examples

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

```
Device# show nat64 prefix stateful global

Global Stateful Prefix: is valid, 2001:DB8::/96
IFs Using Global Prefix    Gi0/1/0
```

The following is sample output from the **show nat64 prefix stateful interfaces** command:

```
Device# show nat64 prefix stateful interfaces
```

```
Stateful Prefixes


Interface               NAT64        Enabled    Global Prefix

GigabitEthernet0/1/0    TRUE          TRUE      2001:DB8:1:1/96
GigabitEthernet0/1/3    TRUE          FALSE     2001:DB8:2:2/96
```

The following is sample output from the **show nat64 prefix stateful static-routes** command:

```
Device# show nat64 prefix stateful static-routes

Stateful Prefixes


NAT64 Prefix    Static Route  Ref-Count

2001:DB8:1:1/96   1
2001:DB8:2:1/96   1
```

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

Table 40: show nat6 prefix stateful Field Descriptions

Field	Description
IFs Using Global Prefix	Lists the interfaces that are using the specified global prefix.
Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Static Route	IPv6 static route that is configured to route packets.

Related Commands

Command	Description
nat64 prefix stateful	Configures a prefix and prefix length for stateful NAT64.

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.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

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.

Examples

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

```
Device# 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 41: 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.

```
Device# 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 42: 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.

```
Device# 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.
15.4(1)T	This command was integrated into Cisco IOS Release 154(1)T.

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.

Examples

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

```
Device# 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 43: show nat64 routes Field Descriptions

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

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

show nat64 services

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Usage Guidelines

Cisco IOS XE Release 3.4S supports only FTP service.

Examples

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

```
Device# show nat64 services

NAT64 Services

ftp
   UDP Enabled: TRUE
   TCP Enabled: TRUE
   Service Definition
   Protocol: 6 Port: 21
```

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

Table 44: show nat64 services Field Descriptions

Field	Description
UDP Enabled	Indicates whether service translation is enabled by default for UDP packets, if the protocol is supported by the service definition.
TCP Enabled	Indicates whether the service translation is enabled by default for TCP packets, if the protocol is supported by the service definition.

Field	Description
Service Definition	The definition of the service (the protocol and port fields for which packets are considered a match to the given service).

Related Commands

Command	Description
nat64 service ftp	Enables NAT64 FTP service.

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* | **limit** | **mapping dynamic**[**acl** *acl-name* **pool** *pool-name* | **pool***pool-name*] | **prefixstateful** *ipv6-prefix/prefix-length* | **stateless**]

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.
limit	(Optional) Clears the statistics for a specific limit. <what is the limit?>
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.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

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.

Examples

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

```
Device# show nat64 statistics

NAT64 Statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Sessions found: 518938
Sessions created: 2
Expired translations: 1
Global Stats:
   Packets translated (IPv4 -> IPv6)
      Stateless: 30
      Stateful: 259469
   Packets translated (IPv6 -> IPv4)
      Stateless: 30
      Stateful: 259471

Interface Statistics
   GigabitEthernet0/1/0 (IPv4 configured, IPv6 not configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 15
         Stateful: 259469
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 0
      Packets dropped: 0
   GigabitEthernet0/1/3 (IPv4 not configured, IPv6 configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 259471
      Packets dropped: 0
Dynamic Mapping Statistics
   v6v4
      access-list mylist pool mypool refcount 2
         pool mypool:
            start 34.1.1.1 end 34.1.1.1
            total addresses 1, allocated 1 (100%)
            address exhaustion packet count 0
Limit Statistics
   max entry: max allowed 200, used 2, packets exceeded 0
```

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

Table 45: 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 nat64 timeouts

To display the Network Address Translation 64 (NAT64) translation session timeout, use the **show nat64 timeouts** command in user EXEC or privileged EXEC mode.

show nat64 timeouts

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

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

```
Device# show nat64 timeouts

NAT64 Timeout
   Seconds     CLI Cfg Uses 'All' all flows
   86400       FALSE   FALSE      udp
   300         FALSE   TRUE       tcp
   7200        FALSE   TRUE       tcp-transient
   240         FALSE   FALSE      icmp
   60          FALSE   TRUE
```

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

Table 46: show nat64 timeouts Field Descriptions

Field	Description
Seconds	NAT64 timeout, in seconds.
CLI Cfg	Indicates whether the timeout is explicitly configured through the CLI. The timeout values configured through the CLI changes the default timeout values.

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.

show nat64 translations

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

show nat64 translations {**port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}} [**total** | **verbose**]

Syntax Description

port	Displays information about NAT64 translations filtered by port numbers.
number	Port number. Valid values are from 1 to 65535.
protocol	Displays information about NAT64 translations, filtered by the protocols configured.
icmp	Displays Internet Control Message Protocol (ICMP) entries.
tcp	Displays TCP entries.
udp	Displays UDP entries.
v4	Displays information about NAT64 translations based on an IPv4 address.
original	Displays translations for the original address.
ipv4-address	IPv4 address.
translated	Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	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.
v6	Displays information about NAT64 translations based on an IPv6 address.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.4(2)T	This command was integrated into Cisco IOS Release 15.4(2)T.

Examples

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

```
Device# show nat64 translations port 23

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822

Total number of translations: 1
```

The following is sample output from the **show nat64 translations v4 original** command:

```
Device# show nat64 translations v4 original 192.0.2.1

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822
icmp   192.0.2.1:2816        [3001::c000:201]:2816
       56.1.1.1:2816         [2001:db8::1]:2816

Total number of translations: 2
```

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

Table 47: show nat64 translations Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations entry-type

To display information about Network Address Translation 64 (NAT64) translations filtered by entry type, use the **show nat64 translations entry-type** command in user EXEC or privileged EXEC mode.

show nat64 translations entry-type {**bind** {**all** | **dynamic** | **static**} | **session**} [**total** | **verbose**]

Syntax Description

bind	Displays information about NAT64 translation mapping entries.
all	Displays information about all NAT64 translation mapping entries.
dynamic	Displays information about dynamic mapping entries.
static	Displays information about static mapping entries.
session	Displays information about NAT64 translation session entries.
total	(Optional) Displays information about the total NAT64 translation entry count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations entry-type session** command:

```
Router# show nat64 translations entry-type session

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

---    ---                   ---
       56.1.1.1              2001:db8::1

Total number of translations: 1
```

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

Table 48: show nat64 translations entry-type session Field Descriptions

Field	Description
Proto	Protocol type.

Field	Description
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations redundancy

To display the Network Address Translation 64 (NAT64) translations filtered by redundancy groups (RGs), use the **show nat64 translations redundancy** command in user EXEC or privileged EXEC mode.

show nat64 translations redundancy *group-id* [**total** | **verbose**]

Syntax Description

group-id	Redundancy group ID. Valid values are from 1 and 2.
total	(Optional) Displays information about the total NAT64 redundancy translations.
verbose	(Optional) Displays detailed NAT64 redundancy translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use the output of the verify the redundancy groups that you have configured.

Examples

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

```
Device# show nat64 translations redundancy 1

  Proto  Original IPv4         Translated IPv4
         Translated IPv6       Original IPv6
 ------------------------------------------------------------------------------

         209.165.201.2:21      [2001:DB8:1::103]:32847

 tcp     10.2.1.11:32863       [2001::3201:10b]:32863
         10.1.1.1:80           [2001::11]:80
 tcp     209.165.201.2:21      [2001:DB8:1::104]:32848
         10.1.1.1:80           [2001::11]:80

 Total number of translations: 3
```

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

Table 49: show nat64 translations redundancy Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays IPv4 addresses that were translated into IPv6 addresses and IPv4 addresses that were translated from IPv6 addresses.

Field	Description
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays IPv6 addresses that were translated into IPv4 addresses and IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.

show nat64 translations time

To display information about Network Address Translation 64 (NAT64) translations filtered by time, use the **show nat64 translations time** command in user EXEC or privileged EXEC mode.

show nat64 translations time {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* [**total** | **verbose**]

Syntax Description

created	Displays translation entries that were created at the specified time.
last-used	Displays the translation entries that were last used at the specified time.
newer-than	Displays translation entries that are newer than the time stamp.
older-than	Displays translation entries that are older than the time stamp.
day	Day of the month. Valid values are from 1 to 31.
month	Month of the year. Valid values are from January to December.
year	Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	Time in hh:mm:ss format.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translations time created newer-than** command:

```
Router# show nat64 translations time created newer-than 20 June 2011 20:00:00

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

       56.1.1.1              2001:db8::1
tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:20822        [2001:db8::1]:20822
icmp   192.0.2.1:2816        [3001::c000:201]:2816
       56.1.1.1:2816         [2001:db8::1]:2816

Total number of translations: 3
```

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

Table 50: show nat64 translations time created newer-than Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations total	Displays information about the total NAT64 translation count.
show nat64 translations verbose	Displays the detailed NAT64 translation information.

show nat64 translations total

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

show nat64 translations total [**entry-type** {**bind** {**all** | **dynamic** | **static**} | **session**} | **port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **time** {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}]

Syntax Description

entry-type	(Optional) Displays information about NAT64 translations filtered by entry type.
bind	(Optional) Displays information about NAT64 translation mapping entries.
all	(Optional) Displays information about all NAT64 translation mapping entries.
dynamic	(Optional) Displays information about dynamic mapping entries.
static	(Optional) Displays information about static mapping entries.
session	(Optional) Displays information about NAT64 translation session entries.
port *number*	(Optional) Displays information about NAT64 translations filtered by port number. Valid values are from 1 to 65535.
protocol	(Optional) Displays information about NAT64 translations filtered by protocol.
icmp	(Optional) Displays information about Internet Control Message Protocol (ICMP) entries.
tcp	(Optional) Displays information about TCP entries.
udp	(Optional) Displays information about UDP entries.
time	(Optional) Displays information about NAT64 translations filtered by time.
created	(Optional) Displays translation entries created at the specified time.
last-used	(Optional) Displays the translation entries that were last used at the specified time.
newer-than	(Optional) Displays translation entries that are newer than the time stamp.
older-than	(Optional) Displays translation entries that are older than the time stamp.
day	(Optional) Day of the month. Valid values are from 1 to 31.
month	(Optional) Month of the year. Valid values are from January to December.
year	(Optional) Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	(Optional) Time in hh:mm:ss format.
v4	(Optional) Displays information about NAT64 translations based on an IPv4 address.
original	(Optional) Displays information about translations for the original IPv4 or IPv6 address.

ipv4-address	(Optional) IPv4 address.
translated	(Optional) Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	(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.
v6	(Optional) Displays information about NAT64 translations based on an IPv6 address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

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

```
Router# show nat64 translations total

Total number of translations: 3
```

The output fields are self-explanatory.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays information about NAT64 translations filtered by entry type.
show nat64 translations time	Displays information about NAT64 translations filtered by time.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations v4

To display Network Address Translation 64 (NAT64) translations based on an IPv4 address, use the **show nat64 translations v4** command in user EXEC or privileged EXEC mode.

show nat64 translation v4 {**original** *ipv4-address* | **translated** *ipv6-address*} **total** | **verbose**

Syntax Description

original	Displays translations for the original IPv4 address.
ipv4-address	IPv4-address.
translated	Displays translations for the translated address.
ipv6-address	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.
total	(Optional) Displays the total NAT64 translation count.
verbose	(Optional) Displays detailed NAT64 translation information.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the**show nat64 translation v4 original** command:

```
Router# show nat64 translation v4 original 112.1.1.10

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------

tcp    112.1.1.10:23         [3001::7001:10a]:23
       56.1.1.2:12656        [2001::2]:12656

Total number of translations: 1
```

The following is sample output from the **show nat64 translations v4 translated**command:

```
Router# show nat64 translations v4 translated 3001::7001:10a

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------
```

```
icmp   112.1.1.10:677        [3001::7001:10a]:677
       56.1.1.2:677          [2001::1b01:10a]:677

Total number of translations: 1
```

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

Table 51: show nat64 translations v4 Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address.

Related Commands

Command	Description
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations port	Displays NAT64 translations filtered by port numbers.
show nat64 translations protocol	Displays NAT64 translations filtered by protocols.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translations total	Displays the total NAT64 translation count.
show nat64 translations v6	Displays NAT64 translations based on an IPv6 address.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations v6

To display Network Address Translation 64 (NAT64) translations based on an IPv6 address, use the **show nat64 translations v4** command in user EXEC or privileged EXEC mode.

show nat64 translations v6 {**original** *ipv6-address* | **translated** *ipv4-address*}[**total** | **verbose**]

Syntax Description

original	Displays translations for the original IPv6 address.
ipv6-address	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.
translated	Displays translations for the translated address.
ipv4-address	IPv4-address.
total	Displays the total NAT64 translation count.
verbose	Displays detailed NAT64 translation information.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is sample output from the **show nat64 translation v6 original** command:

```
Router# show nat64 translations v6 original 2001::2

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

---    ---                   ---
       56.1.1.1              2001::2
tcp    112.1.1.10:23         [3001::7001:10a]:23
       56.1.1.1:38924        [2001::2]:38924

Total number of translations: 2
```

The following is sample output from the **show nat64 translations v6 translated** command:

```
Router# show nat64 translations v6 translated 56.1.1.2

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
```

```
--------------------------------------------------------------------------------

---     ---                     ---
        56.1.1.2                2001::1b01:10a
icmp    112.1.1.10:2370         [3001::7001:10a]:2370
        56.1.1.2:2370           [2001::1b01:10a]:2370

Total number of translations: 2
```

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

Table 52: show nat64 translations v6 Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address.

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations port	Displays NAT64 translations filtered by port numbers.
show nat64 translations protocol	Displays NAT64 translations filtered by protocols.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translation total	Displays the total NAT64 translation count.
show nat64 translations v4	Displays NAT64 translations based on an IPv4 address.
show nat64 translations verbose	Displays detailed NAT64 translation information.

show nat64 translations verbose

To display the detailed Network Address Translation 64 (NAT64) translation information, use the **show nat64 translations verbose** command in user EXEC or privileged EXEC mode.

show nat64 translations verbose [**entry-type** {**bind** {**all** | **dynamic** | **static**} | **session**} | **port** *number* | **protocol** {**icmp** | **tcp** | **udp**} | **time** {**created** | **last-used**} {**newer-than** | **older-than**} *day month year hh*:*mm*:*ss* | **v4** {**original** *ipv4-address* | **translated** *ipv6-address*} | **v6** {**original** *ipv6-address* | **translated** *ipv4-address*}]

Syntax Description

entry-type	(Optional) Displays information about NAT64 translations filtered by entry type.
bind	(Optional) Displays information about NAT64 translation mapping entries.
all	(Optional) Displays information about all NAT64 translation mapping entries.
dynamic	(Optional) Displays information about dynamic mapping entries.
static	(Optional) Displays information about static mapping entries.
session	(Optional) Displays information about NAT64 translation session entries.
port *number*	(Optional) Displays information about NAT64 translations filtered by port number. Valid values are from 1 to 65535.
protocol	(Optional) Displays information about NAT64 translations filtered by protocol.
icmp	(Optional) Displays information about Internet Control Message Protocol (ICMP) entries.
tcp	(Optional) Displays information about TCP entries.
udp	(Optional) Displays information about UDP entries.
time	(Optional) Displays information about NAT64 translations filtered by time.
created	(Optional) Displays translation entries created at the specified time.
last-used	(Optional) Displays the translation entries that were last used at the specified time.
newer-than	(Optional) Displays translation entries that are newer than the time stamp.
older-than	(Optional) Displays translation entries that are older than the time stamp.
day	(Optional) Day of the month. Valid values are from 1 to 31.
month	(Optional) Month of the year. Valid values are from January to December.
year	(Optional) Year. Valid values are from 1993 to 2035.
hh:*mm*:*ss*	(Optional) Time in hh:mm:ss format.
v4	(Optional) Displays information about NAT64 translations based on an IPv4 address.
original	(Optional) Displays information about translations for the original IPv4 or IPv6 address.

ipv4-address	(Optional) IPv4 address.
translated	(Optional) Displays information about translations for the translated IPv4 or IPv6 address.
ipv6-address	(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.
v6	(Optional) Displays information about NAT64 translations based on an IPv6 address.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

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

```
Router# show nat64 translations verbose

Proto  Original IPv4         Translated IPv4
       Translated IPv6       Original IPv6
------------------------------------------------------------------------------

       56.1.1.1              2001:db8::1
         created: 01 Jul 2011 15:27:06, last-used:   ---,
           inactivity-time:     ---
         flags: none
         entry-id: 0000000000, use-count: 3
tcp    192.0.2.1:23          [3001::c000:201]:23
       56.1.1.1:42485        [2001:db8::1]:42485
         created: 01 Jul 2011 15:32:01, last-used:   01 Jul 2011 15:32:04,
           inactivity-time:     00:03:53
         flags: timing-out, syn-in
         entry-id: 0x8ca82cd0, use-count: 1
icmp   192.0.2.1:8552        [3001::c000:201]:8552
       56.1.1.1:8552         [2001:db8::1]:8552
         created: 01 Jul 2011 15:31:23, last-used:   01 Jul 2011 15:31:23,
           inactivity-time:     00:00:11
         flags: none
         entry-id: 0x8ca82c30, use-count: 1
icmp   192.0.2.1:983         [3001::c000:201]:983
       56.1.1.1:983          [2001:db8::1]:983
         created: 01 Jul 2011 15:32:06, last-used:   01 Jul 2011 15:32:06,
           inactivity-time:     00:00:54
         flags: none
         entry-id: 0x8ca82d70, use-count: 1

Total number of translations: 4
```

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

Table 53: show nat64 translations verbose Field Descriptions

Field	Description
Proto	Protocol type.
Original IPv4 Translated IPv6	IPv4 address that was translated as an IPv6 address. **Note** This field displays the IPv4 addresses that were translated into IPv6 addresses and the IPv4 addresses that were translated from IPv6 addresses.
Translated IPv4 Original IPv6	IPv6 address that was translated as an IPv4 address. **Note** This field displays the IPv6 addresses that were translated into IPv4 addresses and the IPv6 addresses that were translated from IPv4 addresses.
created	The date and time when the entry was created.
last-used	The date and time when the entry was last used.

Related Commands

Command	Description
show nat64 translations	Displays information about NAT64 translations.
show nat64 translations entry-type	Displays NAT64 translations filtered by entry type.
show nat64 translations time	Displays NAT64 translations filtered by time.
show nat64 translations total	Displays the total NAT64 translation count.

show nhrp debug-condition

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

show nhrp debug-condition

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show nhrp debug-condition
Peer NBMA addresses under debug are:
1.1.1.1,
Interfaces under debug are:
Tunnel1, Peer Tunnel addresses under debug are:
2.2.2.2,
```

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

Related Commands

Command	Description
debug nhrp condition	Enables the NHRP conditional debugging.

show nhrp group-map

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

show 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
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

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.

Note This command will replace the **show ip nhrp group-map** command in a future release.

Examples

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

```
Device# show nhrp group-map

Interface: Tunnel0
 NHRP group: spoke_group1
  QoS policy: group1_parent
  Transport endpoints using the qos policy: None

 NHRP group: spoke_group2
  QoS policy: group2_parent
  Transport endpoints using the qos policy: None

 NHRP group: spoke_group3
  QoS policy: group3_parent
  Transport endpoints using the qos policy: None
```

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

```
Device# show nhrp group-map test-group-0

Interface: Tunnel0
 NHRP group: tes-group-0
  QoS policy: group3_parent
  Transport endpoints using the qos policy:
  6001::1000:1
```

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

Table 54: show 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.
Transport endpoints using the qos policy	List of transport endpoints using the QoS policy.

Related Commands

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

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 55: 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.
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 hardware qfp feature alg statistics sip

To display Session Initiation Protocol (SIP) application layer gateway (ALG)-specific statistics information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg statistics sip** command in privileged EXEC mode.

show platform hardware qfp feature alg statistics sip [**clear** | **dbl** [**all** | **clear** | **entry** *entry-string* [**clear**]] | **dblcfg** | **l7data** {**callid** *call-id* | **clear**} | **processor** | **timer**]

Syntax Description

clear	(Optional) Clears ALG counters after display.
dbl	(Optional) Displays brief information about all SIP blocked list data.
all	(Optional) Displays all dynamic blocked list entries: blocked list and non blocked list entries.
entry *entry-string*	(Optional) Clears the specified blocked list entry.
dblcfg	(Optional) Displays all SIP blocked list settings.
l7data	(Optional) Displays brief information about all SIP Layer 7 data.
callid *call-id*	(Optional) Displays information about the specified SIP call ID.
processor	(Optional) Displays SIP processor settings.
timer	(Optional) Displays SIP timer settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

This command displays the following error details:

- Session write lock exceeded
- Global write lock exceeded
- Blocked list

This command also displays the following event details:

- Blocked list triggered
- Blocked list timeout

A blocked list is a list of entities that are denied a particular privilege, service, or access.

Examples

The following is sample output from the **show platform hardware qfp active feature alg statistics sip** command:

```
Device#  show platform hardware qfp active feature alg statistics sip
```

```
Events
...
Cr dbl entry:                10   Del dbl entry:                 10
Cr dbl cfg entry:             8   Del dbl cfg entry:              4
start dbl trig tmr:          10   restart dbl trig tmr:        1014
stop dbl trig tmr:           10   dbl trig timeout:            1014
start dbl blk tmr:            0   restart dbl blk tmr:            0
stop dbl blk tmr:             0   dbl blk tmr timeout:            0
start dbl idle tmr:          10   restart dbl idle tmr:         361
stop dbl idle tmr:            1   dbl idle tmr timeout:           9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:             0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:          0
Session wlock ovflw:          0    Global wlock ovflw:            0
Blacklisted:                561
```

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

Table 56: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
CR dbl entry	Number of dynamic blocked list entries.
start dbl blk tmr	Number of events that have started the dynamic blocked list timer.
stop dbl idle tmr	Number of events that have stopped the dynamic blocked list idle timer.
Del dbl entry	Number of dynamic blocked list entries deleted.
restart dbl trig tmr	Number of dynamic blocked list trigger timers restarted.
dbl trig timeout	Number of dynamic blocked list trigger timers timed out.
restart dbl blk tmr	Number of dynamic blocked list timers to be restarted.
dbl idle tmr timeout	Number of dynamic blocked list idle timers timed out.
DoS Errors	Denial of service (DoS) related errors.
Dbl Retmem Failed	Number of dynamic blocked list return memory failures.
DblCfg Retm Failed	Number of dynamic blocked list configuration return memory failures.
Session wlock ovflw	Number of packets that are dropped because the session-level write lock number is exceeded.
Blocked list	Number of packets dropped by dynamic blocked list.
Dbl Malloc Failed	Number of dynamic blocked list memory allocation failures.
DblCfg Malloc Failed	Number of dynamic blocked list configuration memory allocation failures.

Field	Description
Global wlock ovflw	Number of packets dropped because the global-level write-lock number is exceeded.

The following is sample output from the **show platform hardware qfp active feature alg statistics sip dbl entry** command:

```
Device# show platform hardware qfp active feature alg statistics sip dbl entry a4a051e0a4a1ebd

req_src_addr: 10.74.30.189              req_dst_addr: 10.74.5.30
trigger_period:     1000(ms)            block_timeout:       30(sec)
idle_timeout:       60(sec)             dbl_flags: 0x        1
cfg_trig_cnt:        5                  cur_trig_cnt:        0
```

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

Table 57: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
req_src_addr	Source IP address of a SIP request message.
trigger_period	Dynamic blocked list trigger period.
idle_timeout	Dynamic blocked list idle timeout entry.
cfg_trig_cnt	Configured trigger counter.
req_dst_addr	Destination IP address of a SIP request message.
block_timeout	Dynamic blocked list block timeout.
dbl_flags	Dynamic blocked list entry flags.
cur_trig_cnt	Current trigger counter.

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blocked list for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

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.

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.

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.

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.
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.

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
```

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 information about all redundancy groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.

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.

Examples

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

```
Device# 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 58: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current priority of the redundancy 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	Redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	Current role of the device.
Peer Role	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 device has started Redundancy Framework (RF) progression.
RF Domain	Name of the 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.

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 59: show redundancy application if-mgr Field Descriptions

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

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

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.

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 60: show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.
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.

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.
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 running-config mdns-sd policy

To display current running multicast Domain Name System (mDNS) service-policy configuration details for the device or interface, use the **show running-config mdns-sd policy** command in privileged EXEC mode.

show running-config mdns-sd policy {**global** | **interface** *type number*}

Syntax Description

global	Displays current running mDNS service-policy configuration details for the device.
interface *type number*	Displays current running mDNS service-policy configuration details for the specified interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-policy configuration details for the device, use the **show running-config mdns-sd policy global** command form.

To view current running mDNS service-policy configuration details for a specific interface, use the **show running-config mdns-sd policy interface** *type number* command form

Examples

The following is sample output for the **show running-config mdns-sd policy** command.

The current running configuration details for the device is displayed below. The output signifies that the mDNS gateway functionality is enabled on the device, and the designated gateway status is enabled without a Time to Live (TTL) value.

```
Device> enable
Device# show running-config mdns-sd policy global


service-routing mdns-sd
  designated-gateway enable
  service-type-enumeration period 16
```

The current running configuration details for the interface is displayed below. The output given below signifies that the mDNS gateway functionality is enabled on the interface, and the designated gateway status is enabled with a TTL value of 20 minutes.

Examples

Current running configuration details for a device interface

The output given below signifies that the mDNS gateway functionality is enabled on the interface, and the designated gateway status is enabled with a TTL value of 20 minutes.

```
Device> enable
Device# show running-config mdns-sd policy interface ethernet 0/1


service-routing mdns-sd
  designated-gateway enable ttl 20
```

Related Commands

Command	Description
show running-config mdns-sd service-instance	Displays current running mDNS service-instance configuration details.
show running-config mdns-sd service-list	Displays current running mDNS service-list configuration details.

show running-config mdns-sd service-instance

To display current running multicast Domain Name System (mDNS) service-instance configuration details, use the **show running-config mdns-sd service-instance** command in privileged EXEC mode.

show running-config mdns-sd service-instance {**all** | **name** *service-instance-name* **regtype** *service-type* **domain** *name*}

Syntax Description

all	Displays all current running mDNS service-instance configuration details.
name *service-instance-name*	Displays current running mDNS service-instance configuration details for the specified service instance.
regtype *service-type*	Specifies that the service instance is of the specified service type.
domain *name*	Specifies the domain with which the service-instance is being associated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-instance configuration details for all services, use the **show running-config mdns-sd service-instance all** command form.

To view current running mDNS service-policy configuration details for a specific service-instance, use the **show running-config mdns-sd service-instance name** *service-instance-name* command form. To view specific service-instance configuration details, you need to specify the service type and domain name too.

Examples

The following is a sample output for the **show running-config mdns-sd service-instance** command.

The current running mDNS service-instance configuration information for all services is displayed below. The service instance names, the service type and the domain names are displayed in the output.

```
Device> enable
Device# show running-config mdns-sd service-instance all


service-instance mdns-sd service serv2 regtype _tcp._123 domain tcp
 port 55
service-instance mdns-sd service serv1 regtype _tcp._12 domain tcp
```

Examples

Current running mDNS service-instance configuration information for a service instance.

```
Device> enable
Device# show running-config mdns-sd service-instance name serv1 regtype _tcp._12 domain tcp

service-instance mdns-sd service serv1 regtype _tcp._12 domain tcp
```

Related Commands

Command	Description
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.
show running-config mdns-sd service-list	Displays current running mDNS service-list configuration details.

show running-config mdns-sd service-list

To display current running multicast Domain Name System (mDNS) service-list configuration details, use the **show running-config mdns-sd service-list** command in privileged EXEC mode.

show running-config mdns-sd service-list {**all** | **name** *service-list-name* [**sequence-number** *sequence-number*] | **query**}

Syntax Description

all	Displays all current running mDNS service-list configuration details. The details include the service-list name, sequence number, the option that is applied, and associated match statements, if any.
name *service-list-name*	Displays current running mDNS service-list configuration details for the specified service list.
sequence-number *sequence-number*	(Optional) Specifies that the service-list configuration details must be displayed for the specified sequence number. **Note** You must specify the sequence number since more than one sequence number can be associated with the same service-list.
query	Displays current running mDNS service-list query details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.

Usage Guidelines

To view current running mDNS service-list configuration details for all service-lists, use the **show running-config mdns-sd service-list all** command form.

To view current running mDNS service-list configuration details for a specific service-list, use the **show running-config mdns-sd service-list name** *service-list-name* [**sequence-number** *sequence-number*] command form. The keyword-argument pair **sequence-number** *sequence-number* enables you to view the match statements associated with the service-list. The match statements are associated with service-lists for filtering types of service, types of service instances and associated queries, and types of messages such as announcements and queries.

To view queries that are associated with various service-lists, use the **show running-config mdns-sd service-list query** command form.

Examples

The following is a sample output for the **show running-config mdns-sd service-list** command.

The current running mDNS service-list configuration information is displayed below. The service list names, match statements, and the permit or deny option details are displayed in the output.

```
Device> enable
Device# show running-config mdns-sd service-list all
```

```
service-list mdns-sd sl1 permit 2
service-list mdns-sd sl3 deny 10
 match message-type announcement
 match service-type _ipp._tcp
service-list mdns-sd srvc-lst permit 6
```

Examples

Current running mDNS service-list configuration for an active query.

```
Device> enable
Device# show running-config mdns-sd service-list query
```

```
service-list mdns-sd sl2 query
service-list mdns-sd sl-qry query
 service-type ser-type
 service-type _tcp._dom1
service-list mdns-sd sd2 query
```

Related Commands

Command	Description
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.
show running-config mdns-sd service-instance	Displays current running mDNS service-instance configuration details.

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific VPN routing and forwarding (VRF) instance or linked to all VRFs configured on the router, use the **show running-config vrf** command in privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify the name of a VRF configuration, the running configurations of all VRFs on the router are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.5S	This command was modified. The output of the command was modified to display the Network Address Translation (NAT) configuration.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, specify the name of the VRF.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration.
- The routing protocol and static routing configurations associated with the VRF.
- The configuration of interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface.

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 720 bytes
```

```
ip vrf vpn3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
!
interface GigabitEthernet0/0/1
 description connected to nat44-1ru-ce1 g0/0/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 ip nat inside
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn3
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
router bgp 100
 !
 address-family ipv4 vrf vpn3
  redistribute connected
  redistribute static
 exit-address-family
ip nat inside source route-map rm-vpn3 pool shared-pool vrf vpn3 match-in-vrf overload
ip nat pool shared-pool 10.0.0.2 10.0.0.254 prefix-length 24
!
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
.
.
.
end
```

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

Table 61: show running-config vrf Field Descriptions

Field	Description
Current configuration: 720 bytes	Indicates the number of bytes (720) in the VRF vpn3 configuration.
ip vrf vpn3	Indicates the name of the VRF (vpn3) for which the configuration is displayed.
rd 100:1	Identifies the route distinguisher (100:1) for VRF vpn3.
route-target export 100:1 route-target import 100:1	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:1 are exported from VRF vpn3. • Routes tagged with the route-target import 100:1 are imported into VRF vpn3.

Field	Description
interface GigabitEthernet0/0/1	Specifies the interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 172.17.0.1 255.0.0.0	Configures the IP address of the Gigabit Ethernet interface.
ip nat inside	Enables NAT of inside addresses.
router bgp 100	Sets up a BGP routing process for the router with the autonomous system number as 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using the standard IPv4 address prefixes.
redistribute connected	Redistributes routes that are automatically established by the IP on an interface into the BGP routing domain.
ip nat pool	Defines a pool of IP addresses for NAT.
router ospf 101 vrf vpn3	Sets up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configures a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show tech nat

To display NAT data that is useful for troubleshooting. The outpout of **show tech nat** command includes output for the following commands:

- **show clock**
- **show version**
- **show running-config**
- **show ip nat translations total**
- **show ip nat stat**
- **show platform hardware qfp active statistics drop**
- **show platform hardware qfp active feature nat datapath stats**
- **show platform hardware qfp active feature nat datapath basecfg**
- **show platform hardware qfp active feature nat datapath map**
- **show platform hardware qfp active feature nat datapath pool**
- **show platform hardware qfp active feature nat datapath port**
- **show platform hardware qfp active feature nat datapath time**
- **show platform hardware qfp active feature nat datapath hsl**
- **show platform hardware qfp active feature nat datapath rmap**
- **show platform hardware qfp active feature nat datapath limit**
- **show platform hardware qfp active feature nat datapath esp**
- **show platform hardware qfp active feature nat datapath gatein**
- **show platform hardware qfp active feature nat datapath gateout**
- **show platform hardware qfp active feature nat datapath ha**
- **show platform hardware qfp active feature nat datapath nonpat**
- **show platform hardware qfp active feature alg statistics**
- **show platform hardware qfp active datapath utilization**
- **show platform hardware qfp active tcam resource-manager usage**

- **show platform software nat counters**
- **show platform software nat rp active msg-stats**
- **show platform software nat rp active db-stats**

```
show tech nat
```

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.3	This command was introduced.

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6-address*
no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses will not overwrite old ones.

Examples

In the following example, the SIP server IPv6 address 2001:0db8::2 is configured to be returned in the SIP server's IPv6 address list option to clients:

```
sip address 2001:0DB8::2
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*
no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Command Default

No default behavior or values.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names will not overwrite old ones.

Examples

The following example configures the SIP server domain name sip1.cisco.com to be returned in the SIP server's domain name list option to clients:

```
sip domain-name sip1.cisco.com
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

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.

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
```

source-interface (mDNS)

To specify an alternate source interface for outgoing multicast Domain Name System (mDNS) packets on a device, use the **source-interface** command in mDNS configuration mode. To disable the alternate source interface for outgoing mDNS packets on a device, use the **no** form of this command.

source-interface *type number*
no source-interface *type number*

Syntax Description

type	Interface type. Specify the interface that you want to configure as the alternate source interface for outgoing mDNS packets on the device. For more information, use the question mark (?) online help function.
number	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

An alternate source interface for outgoing mDNS packets is not configured on a device.

Command Modes

Multicast DNS configuration (config-mdns)

Command History

Release	Modification
15.2(2)E	This command was introduced.
Cisco IOS XE 3.6E	This command was integrated into the Cisco IOS XE 3.6E release.
15.2(1)SY	This command was integrated into Cisco IOS Release 15.2(1)SY.
Cisco IOS XE Release 3.15S	This command was integrated into the Cisco IOS XE Release 3.15S
15.5(2)S	This command was integrated into Cisco IOS 15.5(2)S Release.

Usage Guidelines

Some devices have interfaces for which no IP address is assigned. If you configure the **source-interface** command on such a device, then the IP address of the source-interface is used when outgoing mDNS service information is transported through the interface with no IP address.

Note Before configuring the alternate mDNS source interface for a device, ensure that the source interface has a valid IP address assigned to it.

Examples

The following example shows you how to specify an interface as an alternate source interface for outgoing mDNS packets on a device:

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# source-interface ethernet 0/1
Device(config-mdns)# exit
```

Related Commands

Command	Description
service-routing mdns-sd	Enables mDNS gateway functionality for a device.
show mdns statistics	Displays mDNS statistics for the specified service-list.
show running-config mdns-sd policy	Displays current running mDNS service-policy configuration details for the device or interface.

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.

Examples

Global Configuration Example

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
```

VPN Configuration Example

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
```

VPN ID Configuration Example

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.

Command	Description
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.

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.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** 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.

trusted-port (DHCPv6 Guard)

To configure a port to become a trusted port, use the **trusted-port** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, messages received on ports that have this policy are not verified.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and sets the port to trusted:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

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.

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.

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.

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.

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:

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.
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.

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.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 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 with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

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

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.