clear ip route dhcp through ip arp entry learn

clear ip route dhcp

To remove routes from the routing table added by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent for the DHCP clients on unnumbered interfaces, use the **clear ip route dhcp**command in EXEC mode.

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

Examples

The following example removes a route to network 10.5.5.217 from the routing table:

```
Router# clear ip route dhcp 10.5.5.217
```

Related Commands

Command	Description
show ip route dhcp	Displays the routes added to the routing table by the Cisco IOS DHCP server and relay agent.

clear ip snat sessions

To clear dynamic Stateful Network Address Translation (SNAT) sessions from the translation table, use the **clear ip snat sessions**command in EXEC mode.

clear ip snat sessions * [ip-address-peer]

Syntax Description

*	Removes all dynamic entries.
ip-address-peer	(Optional) Removes SNAT entries of the peer translator.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example shows the SNAT entries before and after using the **clear ip snat sessions** command:

```
Router> show ip snat distributed
SNAT:Mode PRIMARY
    :State READY
    :Local Address 10.168.123.2
    :Local NAT id 100
    :Peer Address 10.168.123.3
    :Peer NAT id 200
    :Mapping List 10
Router> clear ip snat sessions *
Closing TCP session to peer:10.168.123.3
Router> show ip snat distributed
```

clear ip snat translation distributed

To clear dynamic Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation distributed**command in EXEC mode.

clear ip snat translation distributed *

Syntax Description

*	Removes all dynamic SNAT entries.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example clears all dynamic SNAT translations from the translation table:

```
Router# clear ip snat translation distributed *
```

clear ip snat translation peer

To clear peer Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation peer**command in EXEC mode.

clear ip snat translation peer ip-address-peer [refresh]

Syntax Description

ip-address-peer	IP address of the peer translator.
refresh	(Optional) Provides a fresh dump of the NAT table from the peer.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use this command to clear peer entries from the translation table before they time out.

Examples

The following example shows the SNAT entries before and after the peer entry is cleared:

```
Router# show ip snat peer
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.25.20      192.168.122.20     ---                ---
tcp 192.168.25.20:33528 192.168.122.20:33528 192.168.24.2:21 192.168.24.2:21
Router# clear ip snat translation peer 192.168.122.20
```

clear ip dhcp snooping database statistics

To clear the DHCP binding database statistics, use the **clear ip dhcp snooping database statistics** command in privileged EXEC mode.

clear ip dhcp snooping database statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to clear the statistics from the DHCP binding database:

```
Router# clear ip dhcp snooping database statistics
```

clear ip translation peer

To clear or reset the Network Address Translation (NAT) entries created by the Stateful Failover of Network Address Translation (SNAT) peer router and retreive a list of NAT entries, use the **clear ip translation peer** command in privileged EXEC mode.

clear ip translation peer *ip-address* **refresh**

Syntax Description

ip-address	IP address of the SNAT peer router.
refresh	Retrieves a list of NAT entries from the SNAT peer router.

Command Default

The NAT entries created by the SNAT peer router are recorded.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to retrieve a list of NAT entries and clear the NAT entries created by the SNAT peer router:

```
Router# clear ip translation peer 10.1.1.1 refresh
```

Related Commands

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

clear ipv6 dhcp

To clear IPv6 Dynamic Host Configuration Protocol (DHCP) information, use the **clear ipv6 dhcp**command in privileged EXEC mode:

clear ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example :

```
Router# clear ipv6 dhcp
```

clear ipv6 dhcp binding

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

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

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified. It was updated to allow for clearing all address bindings associated with a client.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)SXE.
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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **clear ipv6 dhcp binding** command is used as a server function.

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

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.

- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table. If the optional **vrf** *vrf-name* keyword and argument combination is used, only the bindings for the specified VRF are cleared.

Examples

The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# clear ipv6 dhcp binding
```

Related Commands

Command	Description
show ipv6 dhcp binding	Displays automatic client bindings from the DHCP for IPv6 server binding table.

clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the **clear ipv6 dhcp client** command in privileged EXEC mode.

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXE.

Usage Guidelines

The **clear ipv6 dhcp client** command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Examples

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Router# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

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

clear ipv6 dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database, use the **clear ipv6 dhcp conflict** command in privileged EXEC mode.

clear ipv6 dhcp conflict {*****| *ipv6-address*| **vrf** *vrf-name*}

Syntax Description

*****	Clears all address conflicts.
ipv6-address	Clears the host IPv6 address that contains the conflicting address.
vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

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.

If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

If the **vrf** *vrf-name* keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Router# clear ipv6 dhcp conflict *
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.

clear ipv6 dhcp-ldra statistics

To clear Lightweight DHCPv6 Relay Agent (LDRA) related statistics, use the **clear ipv6 dhcp-ldra statistics** command in user EXEC or privileged EXEC mode.

clear ipv6 dhcp-ldra statistics [*interface-type number*]

Syntax Description

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

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

The following interfaces are allowed and can be used for the *interface-type* argument:

- FastEthernet
- GigabitEthernet
- Loopback
- Lspvif
- null
- Port-channel
- TenGigabitEthernet
- Tunnel

Examples

The following clears LDRA-related statistics for the GigabitEthernet 0/1 interface:

```
Device> enable
Device# clear ipv6 dhcp-ldra statistics GigabitEthernet 0/1
Device# exit
```

Related Commands

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

clear ipv6 dhcp relay binding

To clear an IPv6 address or IPv6 prefix of a Dynamic Host Configuration Protocol (DHCP) for IPv6 relay binding, use the **clear ipv6 dhcp relay binding** command in privileged EXEC mode.

clear ipv6 dhcp relay binding{**vrf** *vrf-name*} {*| *ipv6-address*| *ipv6-prefix*}

Cisco uBR10012 and Cisco uBR7200 Series Universal Broadband Devices

clear ipv6 dhcp relay binding{**vrf** *vrf-name*} {*| *ipv6-prefix*}

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
15.2(1)S	The command was modified to delete the binding or route for IPv6 addresses.
Cisco IOS XE Release 3.5S	The command was modified to delete the binding or route for IPv6 addresses.
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

The **clear ipv6 dhcp relay binding** command deletes a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding. If no relay client is specified, no binding is deleted.

Examples

The following example shows how to clear the binding for a client with a specified IPv6 address:

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

The following example shows how to clear the binding for a client with the VRF name vrf1 and a specified prefix on a Cisco uBR10012 universal broadband device:

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

Related Commands

Command	Description
show ipv6 dhcp relay binding	Displays DHCPv6 IANA and DHCPv6 IAPD bindings on a relay agent.

clear ipv6 dhcp route

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

clear ipv6 dhcp route {**vrf** *vrf-name*} {*| *ipv6-address*| *ipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Clears all DHCPv6 added routes.
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 example shows how to clear routes added by DHCPv6 on a DHCPv6 server for IANA and IAPD:

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

Related Commands

Command	Description
show ipv6 dhcp route	Displays the routed added by DHCPv6 on the DHCPv6 server for IANA and IAPD.

clear ipv6 nat translation

To clear dynamic Network Address Translation--Protocol Translation (NAT-PT) translations from the dynamic state table, use the **clear ipv6 nat translation**command in privileged EXEC mode.

clear ipv6 nat translation *

Syntax Description

*	Clears all dynamic NAT-PT translations.

Command Default

Entries are deleted from the dynamic translation state table when they time out.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command to clear entries from the dynamic translation state table before they time out. Static translation configuration is not affected by this command.

Examples

The following example shows the NAT-PT entries before and after the dynamic translation state table is cleared. Note that all the dynamic NAT-PT mappings are cleared, but the static NAT-PT configurations remain.

```
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
Router# clear ipv6 nat translation *
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
```

Related Commands

Command	Description
ipv6 nat	Designates that traffic originating from or destined for the interface is subject to NAT-PT.
show ipv6 nat translations	Displays active NAT-PT translations.

clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command in privileged EXEC mode.

clear logging ip access-list cache

Syntax Description

This command has no arguments or keywords.

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(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.

Examples

This example shows how to clear all the entries from the OAL cache and send them to the syslog:

```
Router#
clear logging ip access-list cache
```

Related Commands

Command	Description
logging ip access-list cache (global configuration)	Configures the OAL parameters globally.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

clear mdns cache

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

clear mdns cache

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **clear mdns cache** command clears mDNS cache information corresponding to all the interfaces on the device, including all mDNS records in cache.

Examples

The following example shows how to clear mDNS cache information on a device:

```
Device> enable
Device# clear mdns cache
Device# exit
```

Related Commands

Command	Description
show mdns cache	Displays mDNS cache information.

clear mdns statistics

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

clear mdns statistics {**all** | **service-policy** {**all** | **interface** *type number*}}

Syntax Description

all	Clears mDNS statistics for the device or service-policy.
service-policy	Clears mDNS service-policy statistics.
interface *type number*	Clears mDNS service-policy statistics for the specified interface.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to clear mDNS cache information on a device:

```
Device> enable
Device# clear mdns statistics
Device# exit
```

Related Commands

Command	Description
show mdns statistics	Displays mDNS statistics.

clear nat64 ha statistics

To clear the Network Address Translation 64 (NAT64) high availability (HA) statistics, use the **clear nat64 ha statistics** command in privileged EXEC mode.

clear nat64 ha statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The HA statistics include the number of HA messages that are transmitted and received by the Route Processor (RP).

Examples

The following example shows how to use the **clear nat64 ha statistics** command to clear the NAT64 HA statistics:

```
Router# clear nat64 ha statistics
```

Related Commands

Command	Description
show nat64 ha status	Displays information about the NAT64 HA state.

clear nat64 statistics

To clear the Network Address Translation 64 (NAT64) statistics, use the **clear nat64 statistics** command in privileged EXEC mode.

clear nat64 statistics [**failure**| **global**| **interface** *type number*| **limit global**| **pool** *pool-name*| **prefix** [**stateful** *ipv6-prefix*/*prefix-length*| **stateless** [**v4v6**| **v6v4**] *ipv6-prefix*/*prefix-length*]]

Syntax Description

failure	(Optional) Clears NAT64 failure count statistics.
global	(Optional) Clears global NAT64 statistics.
interface	(Optional) Clears interface statistics.
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 about the maximum number of stateful NAT64 translations allowed on a router.
pool *pool-name*	(Optional) Clears statistics for a specified pool.
prefix	(Optional) Clears statistics for a specified prefix.
stateful	(Optional) Clears stateful NAT64 statistics.
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.
stateless	(Optional) Clears stateless NAT64 statistics.
v4v6	(Optional) Clears statistics about the IPv4 address that is associated with an IPv6 host for NAT64.

v6v4	(Optional) Clears statistics about the IPv6 address that is associated with an IPv4 host for NAT64.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The **failure**, **pool**, **stateful**, **stateless**, **v4v6**, and **v6v4** keywords and the *pool-name* argument were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

You can use the **clear nat64 statistics** command to clear the statistics of a specified interface or all the interfaces for a given stateful or stateless prefix.

Examples

The following example shows how to clear NAT64 statistics:

```
Device# clear nat64 statistics
```

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 statistics	Displays statistics about NAT64 interfaces and the translated and dropped packet count.

clear nat64 translations

To clear dynamic stateful Network Address Translation 64 (NAT64) translations, use the **clear nat64 translations** command in privileged EXEC mode.

clear nat64 translations {**all** | **redundancy** *group-id*| **protocol** {**icmp** | **tcp** | **udp**}}

Syntax Description

all	Clears all NAT64 translations.
redundancy *group-id*	Clears translations that are filtered on the basis of the specified redundancy group ID. Valid values are 1 and 2.
protocol	Clears translations that are filtered on the basis of the specified protocol.
icmp	Clears NAT64 Internet Control Message Protocol (ICMP) translations.
tcp	Clears NAT64 TCP translations.
udp	Clears NAT64 UDP translations.

Command Modes

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 **redundancy** *group-id* keyword-argument pair and the **protocol** and **icmp** keywords were added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example shows how to clear all NAT64 translations:

```
Device# clear nat64 translations all
```

The following example shows how to clear translations that are filtered for redundancy group ID 1:

```
Device# clear nat64 translations redundancy 1
```

Related Commands

Command	Description
nat64 translation	Enables NAT64 translation.

client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** command in DHCP pool configuration mode. To delete the client identifier, use the **no** form of this command.

client-identifier *unique-identifier*

no client-identifier

Syntax Description

unique-identifier	The distinct identification of the client in 7- or 27-byte dotted hexadecimal notation. See the "Usage Guidelines" section for more information.

Command Default

No client identifier is specified.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid for manual bindings only. DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. You can specify the unique identifier for the client in either of the following ways:

- A 7-byte dotted hexadecimal notation. For example, 01b7.0813.8811.66, where 01 represents the Ethernet media type and the remaining bytes represent the MAC address of the DHCP client.
- A 27-byte dotted hexadecimal notation. For example, 7665.6e64.6f72.2d30.3032.342e.3937.6230.2e33.3734.312d.4661.302f.31. The equivalent ASCII string for this hexadecimal value is vendor-0024.97b0.3741-fa0/1, where vendor represents the vendor, 0024.97b0.3741 represents the MAC address of the source interface, and fa0/1 represents the source interface of the DHCP client.

For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, *Assigned Numbers*.

You can determine the client identifier by using the **debug ip dhcp server packet** command.

Examples

The following example specifies the client identifier for MAC address 01b7.0813.8811.66 in dotted hexadecimal notation:

```
Device(dhcp-config)# client-identifier 01b7.0813.8811.66
```

Related Commands

Command	Description
hardware-address	Specifies the hardware address of a BOOTP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

client-name

To specify the name of a Dynamic Host Configuration Protocol (DHCP) client, use the **client-name** command in DHCP pool configuration mode. To remove the client name, use the **no** form of this command.

client-name *name*

no client-name

Syntax Description

name	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name abc should not be specified as abc.cisco.com.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	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 client name should not include the domain name.

Examples

The following example specifies a string client1 that will be the name of the client:

```
client-name client1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.

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

control

To configure the control interface type and number for a redundancy group, use the **control**command in redundancy application group configuration mode. To remove the control interface for the redundancy group, use the **no** form of this command.

control *interface-type interface-number* **protocol** *id*

no control

Syntax Description

interface-type	Interface type.
interface-number	Interface number.
protocol	Specifies redundancy group protocol media.
id	Redundancy group protocol instance. The range is from 1 to 8.

Command Default

The control interface is not configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

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

Examples

The following example shows how to configure the redundancy group protocol media and instance for the control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol
 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
data	Configures the data interface type and number 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.

data

To configure the data interface type and number for a redundancy group, use the **data**command in redundancy application group configuration mode. To remove the configuration, use the **no** form of this command.

data *interface-type interface-number*

no data *interface-type interface-number*

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Default

No data interface is configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

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

Usage Guidelines

Use the **data** command to configure the data interface. The data interface can be the same physical interface as the control interface.

Examples

The following example shows how to configure the data Gigabit Ethernet interface for group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.

Command	Description
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.

ddns (DDNS-update-method)

To specify an update method for address (A) Resource Records (RRs) as IETF standardized Dynamic Domain Name System (DDNS), use the **ddns**command in DDNS-update-method configuration mode. To disable the DDNS method for updating, use the **no** form of this command.

ddns [both]

no ddns

Syntax Description

both	(Optional) Both A and PTR RRs are updated.

Command Default

No DDNS updating is configured.

Command Modes

DDNS-update-method 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 Dynamic Host Configuration Protocol (DHCP) is used to configure the IP address on the interface, a DHCP client may not perform both A and PTR RRs or any updates. Also, if the DHCP server notifies the client during the DHCP interaction that it will perform the updates, then the DHCP client will not perform the updates. The DHCP server can always override the client even if the client is configured to perform the updates.

If the interface is configured using DHCP and if the DDNS update method is configured on that interface, then the DHCP fully qualified domain name (FQDN) option is included in the DHCP packets between the client and the server. The FQDN option contains the hostname, which is used in the update as well as information about what types of updates the client has been configured to perform.

If the **ddns** keyword is specified, the A RRs only are updated, but if the **ddns both** keyword are specified, both the A and the PTR RRs are updated. Also, if the DHCP server returns the the FQDN option with an updated hostname, that hostname is used in the update instead.

Examples

The following example shows how to configure a DHCP server to perform both A and PTR RR updates:

```
ip ddns update method unit-test
 ddns both
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

default-mapping-rule

To configure Network Address Translation 64 (NAT64) mapping of addresses and ports translation (MAP-T) default domain mapping rule, use the **default-mapping-rule** command in NAT64 MAP-T configuration mode. To remove the NAT64 MAP-T default domain mapping rule, use the **no** form of this command.

default-mapping-rule*ipv6-prefix*/*prefix-length*

no default-mapping-rule

Syntax Description

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

Command Default

Command Modes

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

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 example shows how to configure a default domain mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# default-mapping-rule 2001:0DB8:0:1::/64
```

Related Commands

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

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2 ... address8*]

no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the default router:

```
default-router 10.12.1.99
```

Related Commands

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

device-role (DHCPv6 Guard)

To specify the role of the device attached to the target (which can be an interface or VLAN), use the **device-role** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To remove the specification, use the **no** form of this command.

device-role {**client**| **server**}

no device-role

Syntax Description

client	Sets the role of the device to client.
server	Sets the role of the device to server.

Command Default

The device role is client.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

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

Usage Guidelines

The **device-role** command specifies the role of the device attached to the target (which can be an interface or VLAN) . The device role is primarily used to allow and disallow DHCP replies and DHCP advertisements when they are received on an interface with a device role other than server or relay.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and configures the device as the server:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# device-role server
```

Related Commands

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

dns forwarder

To add an address to the end of the ordered list of IP addresses for a Domain Name System (DNS) view to use when forwarding incoming DNS queries, use the **dns forwarder** command in DNS view configuration mode. To remove an IP address from the list, use the **no** form of this command.

dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*

no dns forwarder [**vrf** *vrf-name*] *forwarder-ip-address*

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance of the *forwarder-ip-address*. **Note** If no VRF is specified, the default is the global VRF.
forwarder-ip-address	IP address to use when forwarding DNS queries handled using the DNS view. **Note** You can specify an IPv4 or IPv6 address for the forwarder IP address.

Command Default

Provided that DNS forwarding (configured by using the **dns forwarding** command) is enabled and the interface to use when forwarding incoming DNS queries is configured (if using the **dns forwarding source-interface** command) and not shut down, incoming DNS queries handled using the DNS view are forwarded to one of the DNS forwarding name servers.

If no forwarding name servers are configured for the DNS view, the device uses any configured domain name server addresses.

If there are no domain name server addresses configured either, the device forwards incoming DNS queries to the limited broadcast address (255.255.255.255) so that the queries are received by all hosts on the local network segment but not forwarded by devices.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *forwarder-ip-address* argument.

Usage Guidelines

This command can be entered multiple times to specify a maximum of six forwarding name servers. After six forwarding name servers have been specified, additional forwarding name servers cannot be specified unless an existing entry is removed.

To display the list of DNS forwarding name server addresses configured for the DNS view, use the **show ip dns view** command.

Note DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view). Earlier to this command being introduced, the resolving name server list was used for resolving internal DNS queries and forwarding DNS queries received by the DNS server. For backward compatibility, if there are no forwarding name servers configured, the resolving name server list will be used instead.

Examples

The following example shows how to add three IP addresses to the list of forwarder addresses for the DNS view named user3 that is associated with the VRF vpn32:

```
Device(config)# ip dns view vrf vpn32 user3
Device(cfg-dns-view)# dns forwarder 192.168.2.0
Device(cfg-dns-view)# dns forwarder 192.168.2.1
Device(cfg-dns-view)# dns forwarder 192.168.2.2
```

The following example shows how to add the IP address 192.0.2.3 to the list of forwarder addresses for the DNS view named user1 that is associated with the VRF vpn32, with the restriction that incoming DNS queries will be forwarded to 192.0.2.3 only if the queries are from the VRF named vpn1:

```
Device(config)# ip dns view vrf vpn32 user1
Device(cfg-dns-view)# dns forwarder vrf vpn1 192.168.2.3
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.

Command	Description
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns forwarding

To enable forwarding of incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding** command in DNS view configuration mode. To disable forwarding and revert to the default configuration, use the **no** form of this command.

dns forwarding [**retry** *number*| **timeout** *seconds*]

no dns forwarding [**retry**| **timeout**]

Syntax Description

retry	(Optional) Specifies the time to retry forwarding a DNS query.
number	(Optional) Number of retries. The range is from 0 to 100.
timeout	(Optional) Specifies the timeout waiting for response to a forwarded DNS.
seconds	(Optional) Timeout in seconds. The range is from 1 to 3600.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global configuration command. However, the **dns forwarding** command for the DNS view does not have a reciprocal side effect on the setting configured by the **ip domain lookup** command.

Command Modes

DNS view configuration (cfg-dns-view)

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.0(1)M	This command was modified. The **retry** *number* and **timeout** *seconds* keywords and arguments were added.

Usage Guidelines

This command enables forwarding of incoming DNS queries handled using the DNS view.

To display the DNS forwarding setting for a DNS view, use the **show ip dns view** command.

If you configure the **no domain lookup** command for a DNS view while the **dns forwarding** command has not been disabled for that view, then the **dns forwarding** command setting will appear in the **show ip dns view** command output in order to make it clear that DNS forwarding is still enabled.

If you configure the **no ip domain lookup** global configuration command, however, the **no dns forwarding** setting is automatically configured also, in order to be backward compatible with the global command form.

Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view. By default, domain lookup and DNS forwarding are both enabled for a view. If you then configure the **no domain lookup**command, DNS forwarding is still enabled. However, if you instead use the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global configuration command.

Examples

The following example shows how to enable forwarding of incoming DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# dns forwarding
```

Related Commands

Command	Description
dns forwarding source-interface	Specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns forwarding source-interface

To specify the interface to use when forwarding incoming Domain Name System (DNS) queries handled using the DNS view, use the **dns forwarding source-interface** command in DNS view configuration mode. To remove the specification of the source interface for a DNS view to use when forwarding DNS queries, use the **no** form of this command.

dns forwarding source-interface *interface*

no dns forwarding source-interface

Syntax Description

interface	Router interface to use when forwarding DNS queries.

Command Default

No interface is specified for forwarding incoming DNS queries handled using the DNS view, so the router selects the appropriate source IP address automatically, according to the interface used to send the packet, when the query is forwarded.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command specifies the interface to use when forwarding incoming DNS queries handled using the DNS view.

To display the interface configured by this command, use the **show ip dns view** command.

Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **dns forwarding source-interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
```

```
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface              IHQ    IQD  OHQ    OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------------
* FastEthernet0/0          0     0    0      0     0    0     0    0     0
  FastEthernet0/1          0     0    0      0     0    0     0    0     0
  ATM2/0                   0     0    0      0     0    0     0    0     0
  Ethernet3/0              0     0    0      0     0    0     0    0     0
  Ethernet3/1              0     0    0      0     0    0     0    0     0
  Ethernet3/2              0     0    0      0     0    0     0    0     0
  Ethernet3/3              0     0    0      0     0    0     0    0     0
  ATM6/0                   0     0    0      0     0    0     0    0     0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to configure FastEthernet slot 0, port 1 as the interface to be used to forward DNS queries for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# dns forwarder source-interface FastEthernet0/1
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
show interfaces	Display statistics for all interfaces configured on the router or access server.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2 ... address8*]

no dns-server

Syntax Description

address	The IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	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

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
dns-server 10.12.1.99
```

Related Commands

Command	Description
domain-name (DHCP)	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dns-server (config-dhcp-global-options)

To configure the Domain Name System (DNS) servers that are available to DHCP clients on request, use the **dns-server** command in DHCP global options configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ip-address* [*ip-address2...ip-address8*]

no dns-server

Syntax Description

ip-address	IP address of a DNS server.
ip-address2...ip-address8	(Optional) IP address of DNS servers. You can specify up to eight IP addresses.

Command Default

If DNS servers are not configured for a DHCP client, the client cannot correlate hostnames to IP addresses.

Command Modes

DHCP global options configuration (config-dhcp-global-options)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

Before you configure the **dns-server** command, you must enter DHCP global options configuration mode by using the **ip dhcp global-options** command.

Examples

The following example shows how to configure two DNS servers:

```
Router(config)# ip dhcp global-options
Router(config-dhcp-global-options)# dns-server 192.0.2.1 192.168.2.1
```

Related Commands

Command	Description
ip dhcp global-options	Enters DHCP global options configuration mode, which is used to configure DHCP-related global configurations.

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This 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

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

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.

Command History

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

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

domain list

To add a domain name to the end of the ordered list of domain names used to complete unqualified hostnames (names without a dotted-decimal domain name) in Domain Name System (DNS) queries handled using the DNS view, use the **domain list** command in DNS view configuration mode. To remove a name from the domain search list, use the **no** form of this command.

domain list *domain-name*

no domain list *domain-name*

Syntax Description

domain-name	Domain name to add or delete from the domain search list. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain list is defined for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command adds a domain name to the end of the domain search list for the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the list of domain names used to complete unqualified hostnames in DNS queries received by a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to add two domain names to the list for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain list example1.com
Router(cfg-dns-view)# domain list example1.org
```

The following example shows how to add two domain names to the list for the DNS view and then delete one of the domain names from the list:

```
Router(cfg-dns-view)# domain list example2.com
Router(cfg-dns-view)# domain list example2.org
Router(cfg-dns-view)# no domain list example2.net
```

Related Commands

Command	Description
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain lookup

To enable the IP Domain Name System (DNS)-based hostname-to-address translation for internally generated DNS queries handled using the DNS view, use the **domain lookup** command in DNS view configuration mode. To disable domain lookup for hostname resolution, use the **no** form of this command.

domain lookup

no domain lookup

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is inherited from the global setting configured using the **ip domain lookup** global command. However, the **domain lookup** DNS view command does not have a reciprocal side effect on the setting configured by the **ip domain lookup** global command.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.

To display the DNS lookup setting for a DNS view, use the show ip dns view command.

If you configure **no dns forwarding** for a DNS view while **domain lookup** has not been disabled for that view, then the **domain lookup** setting will appear in the **show ip dns view** command output in order to make it clear that domain lookup is still enabled.

If you configure the **no ip domain lookup** global command, however, the **no domain lookup** setting is automatically configured also, in order to be backward compatible with the global command form.

Note DNS lookup and DNS forwarding are configured separately. The **domain lookup** command enables the resolution of internally generated DNS queries handled using the DNS view. The **dns forwarding** command enables the forwarding of incoming DNS queries handled using the DNS view. By default, both domain lookup and DNS forwarding are both enabled for a view. If you then configure **no domain lookup**, DNS forwarding is still enabled. However, if you instead uses the older Cisco IOS command **no ip domain lookup** to disable domain lookup for the global default view, then DNS forwarding is disabled automatically. This is done for backward compatibility with the functionality of the **no ip domain lookup** global command.

Examples

The following example shows how to enable IP DNS-based hostname-to-address translation in the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain lookup
```

Related Commands

Command	Description
dns forwarding	Enables forwarding of incoming DNS queries by the DNS view.
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the router can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain multicast

To configure the domain name to be used when performing multicast address lookups for internally generated Domain Name System (DNS) queries handled using the DNS view, use the **domain multicast** command in DNS view configuration mode. To remove the specification of the domain name for multicast address lookups, use the **no** form of this command.

domain multicast *domain-name*

no domain multicast

Syntax Description

domain-name	Domain name to be used when performing multicast address lookups.

Command Default

No IP address is specified for performing multicast address lookups for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the domain name to be used when performing multicast address lookups for internally generated DNS queries handled using the DNS view.

To display the domain name for multicast address lookups, use the **show ip dns view** command.

Examples

The following example shows how to configure the domain name www.example.com as the domain name to be used when performing multicast lookups for internally generated DNS queries handled using the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain multicast www.example.com
```

Related Commands

Command	Description
ip domain multicast	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.

Command	Description
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain name

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain name** command in DNS view configuration mode. To remove the specification of the default domain name for a DNS view, use the **no** form of this command.

domain name *domain-name*

no domain name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the default domain name used to complete unqualified hostnames in DNS queries handled using the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the default domain name configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to define example.com as the default domain name for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain name example.com
```

Related Commands

Command	Description
domain list	Defines the ordered list of default domain names to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client, use the **domain-name**command in DHCPv6 pool configuration mode. To return to the default for this command, use the **no** form of this command.

domain-name *domain-name*

no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

Release	Modification
12.4(9)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.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the domain-name command in IPv6 configure a domain name for a DHCPv6 client.

Examples

The following example configures a domain name for a DHCPv6 client:

```
Router(config)# ipv6 dhcp pool pool1
Router(cfg-dns-view)# domain-name domainv6
```

domain name-server

To add a name server to the list of Domain Name System (DNS) name servers to be used for a DNS view to resolve internally generated DNS queries, use the **domain name-server** command in DNS view configuration mode. To remove a DNS name server from the list, use the **no** form of this command.

domain name-server [**vrf** *vrf-name*] *name-server-ip-address*

no domain name-server [**vrf** *vrf-name*] [*name-server-ip-address*]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance of the *forwarder-ip-address*. **Note** If no VRF is specified, the default is the global VRF.
name-server-ip-address	IP address of a DNS name server. **Note** You can specify an IPv4 or IPv6 address for the DNS name server.

Command Default

No IP address is explicitly added to the list of resolving name servers for this view, although an IP address can be added to the list if dynamic name server acquisition is enabled. If the list of resolving name servers is empty, the device will send the query to the limited broadcast address 255.255.255.255 when this view is used.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.4(1)T	This command was modified. An IPv6 address can be specified for the *name-server-ip-address* argument.

Usage Guidelines

This command can be entered multiple times to specify a maximum of six resolving name servers. After six resolving name servers have been specified, additional resolving name servers cannot be specified unless an existing entry is removed.

This method of explicitly populating the list of resolving name servers is useful in an enterprise network where the population of available DNS servers is relatively static. In an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently, the device can learn a DNS server address through either DHCP or PPP on the interface. To configure the dynamic acquisition of DNS resolving

name server addresses, use the **domain name-server interface** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

To display the list of DNS resolving name server IP addresses configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries for the DNS view). If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.

Examples

The following example shows how to specify the hosts at 192.168.2.111 and 192.168.2.112 as the name servers for the DNS view named user3 that is associated with the VRF vpn32:

```
Device(config)# ip dns view vrf vpn32 user3
Device(cfg-dns-view)# domain name-server 192.168.2.111
Device(cfg-dns-view)# domain name-server 192.168.2.112
```

Related Commands

Command	Description
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view.
domain name-server interface	Specifies the interface from which the device can learn (through either DHCP or PPP interaction on the interface) a DNS resolving name server address for the DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain name-server interface

To specify the interface on which the router can learn (through either DHCP or PPP) Domain Name System (DNS) a resolving name server address for the DNS view, use the **domain name-server interface** command in DNS view configuration mode. To remove the definition of the interface, use the **no** form of this command.

domain name-server interface *interface*

no domain name-server interface *interface*

Syntax Description

interface	Interface on which to acquire the IP address of a DNS name server that the DNS view can use to resolve internally generated DNS queries. The interface must connect to another router on which the DHCP agent or the PPP agent has been configured to allocate the IP address of the DNS server.

Command Default

No interface is used to acquire the DHCP or PPP address to be used for a DNS view to resolve internally generated DNS queries.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command specifies the interface from which to acquire (through DHCP or PPP interaction on the interface) the IP address of a DNS server to add to the list of DNS name servers used to resolve internally generated DNS queries for the DNS view.

The dynamic acquisition of DNS resolving name server addresses is useful in an Internet service provider (ISP) environment, where primary and secondary DNS server addresses can change frequently. To explicitly populate the list of resolving name servers in an enterprise network where the population of available DNS servers is relatively static, use the **domain name-server** command. Regardless of the method or methods used to populate the list of DNS resolving name servers for the view, no more than six resolving name servers are maintained for the view.

Note The DNS resolving name servers and DNS forwarding name servers are configured separately. The **domain name-server** and **domain name-server interface** commands are used to specify the DNS resolving name servers (the ordered list of IP addresses to use when resolving internally generated DNS queries for the DNS view). The **dns forwarder** command specifies the forwarder addresses (the ordered list of IP addresses to use when forwarding incoming DNS queries for the DNS view). If there is no DNS forwarder configuration in a view, then the domain name server list will be used when forwarding DNS queries. This is done for backward compatibility with the **ip name-server** global command.

Tip To list all the interfaces configured on the router or access server, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface* argument in the **domain name-server interface** command.

Examples

The following is sample output from the **show interfaces** command used with the **summary** keyword:

```
Router# show interfaces summary
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0     0    0     0    0    0
  FastEthernet0/1          0     0    0     0     0    0     0    0    0
  ATM2/0                   0     0    0     0     0    0     0    0    0
  Ethernet3/0              0     0    0     0     0    0     0    0    0
  Ethernet3/1              0     0    0     0     0    0     0    0    0
  Ethernet3/2              0     0    0     0     0    0     0    0    0
  Ethernet3/3              0     0    0     0     0    0     0    0    0
  ATM6/0                   0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

The following example shows how to specify a list of name servers for the DNS view named user3 that is associated with the VRF vpn32. First, the list of name server addresses is cleared, then five DNS server IP addresses are added to the list. Finally, FastEthernet slot 0, port 0 is specified as the interface on which to acquire, by DHCP or PPP interaction, a sixth DNS server IP address.

```
Router(config)# ip dns view vrf vpn32 user3

Router(cfg-dns-view)# no domain name-server

Router(cfg-dns-view)# domain name-server 192.168.2.1

Router(cfg-dns-view)# domain name-server 192.168.2.2

Router(cfg-dns-view)# domain name-server 192.168.2.3

Router(cfg-dns-view)# domain name-server 192.168.2.4

Router(cfg-dns-view)# domain name-server 192.168.2.5

Router(cfg-dns-view)# domain name-server interface FastEthernet0/0
```

Related Commands

Command	Description
domain name-server	Specifies the ordered list of IP addresses to use when resolving internally generated DNS queries handled using the DNS view.
show interfaces	Display statistics for all interfaces configured on the router or access server.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain resolver source-interface

To set the source IP address of the Domain Name Server (DNS) queries for the DNS resolver functionality, use the **domain resolver source-interface** command in DNS view configuration mode. To disable the configuration, use the **no** form of this command.

domain resolver source-interface *interface-type number*

no domain resolver source-interface

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

Disabled. (DNS queries are not forwarded through the expected interface.)

Command Modes

DNS view configuration (cfg-dns-view)

Command History

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

Usage Guidelines

Sometimes, when a source interface is configured on a router with the split DNS feature to forward DNS queries, the router does not forward the DNS queries through the configured interface. If you want the router to forward the DNS queries through a particular source interface, configure the router using the **domain resolver source-interface** command.

Examples

The following example shows how to set the source IP address of the DNS queries for the DNS resolver functionality:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain resolver source-interface fastethernet 0/0
```

Related Commands

Command	Description
ip dns view	Creates the DNS view of the specified name associated with the specified VRF instance and then enters DNS view configuration mode.

domain retry

To configure the number of retries to perform when sending or forwarding Domain Name System (DNS) queries handled using the DNS view, use the **domain retry** command in DNS view configuration mode. To remove the specification of the number of retries for a DNS view, use the **no** form of this command.

domain retry *number*

no domain retry

Syntax Description

number	Number of times to retry sending or forwarding a DNS query. The range is from 0 to 100.

Command Default

number : 2 times

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the number of retries to perform when sending or forwarding DNS queries handled using the DNS view.

To display the number of retries configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to send out or forward ten DNS queries from the DNS view named user3 that is associated with the VRF vpn32 before giving up:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain retry 10
```

Related Commands

Command	Description
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain round-robin

To enable round-robin rotation of multiple IP addresses associated with a name in the hostname cache used by the DNS view, use the **domain round-robin** command in DNS view configuration mode. To disable round-robin functionality for the DNS view, use the **no** form of this command.

domain round-robin

no domain round-robin

Syntax Description

This command has no arguments or keywords.

Command Default

Round-robin rotation of multiple IP addresses associated with a name in the hostname cache is disabled for the DNS view.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables round-robin rotation such that each time a hostname in the internal cache is accessed, the system returns the next IP address in the cache, rotated such that the second IP address in the list becomes the first one and the first one is moved to the end of the list. For a more detailed description of round-robin functionality, see the description of the **ip domain round-robin** global command in the *Cisco IOS IP Addressing Services Command Reference* .

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command. To define static hostname-to-address mappings in the global hostname cache or VRF hostname cache for the specified DNS view, use the **ip host** command. To display the round-robin setting for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to define the hostname www.example.com with three IP addresses and then enable round-robin rotation for the default DNS view associated with the global VRF. Each time that hostname is referenced internally or queried by a DNS client sending a query to the Cisco IOS DNS server on this system, the order of the IP addresses associated with the host www.example.com will be changed. Because most client applications look only at the first IP address associated with a hostname, this results in different clients using each of the different addresses and thus distributing the load among the three different IP addresses.

```
Router(config)# ip host view www.example.com 192.168.2.100 192.168.2.200 192.168.2.250
Router(config)# ip dns view default
Router(cfg-dns-view)# domain lookup
```

```
Router(cfg-dns-view)# domain round-robin
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip domain round-robin	Enables round-robin functionality on DNS servers.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain timeout

To configure the number of seconds to wait for a response to a Domain Name System (DNS) query sent or forwarded by the DNS view, use the **domain timeout** command in DNS view configuration mode. To remove the specification of the number of seconds for a DNS view to wait, use the **no** form of this command.

domain timeout *seconds*

no domain timeout

Syntax Description

seconds	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600.

Command Default

number : 3 seconds

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command configures the number of seconds to wait for a response to a DNS query sent or forwarded by the DNS view.

To display the number of seconds configured for the DNS view, use the **show ip dns view** command.

Examples

The following example shows how to configure the router to wait 8 seconds for a response to a DNS query received in the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain timeout 8
```

Related Commands

Command	Description
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

domain-name (DHCP)

To specify the domain n ame for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

domain-name *domain*

no domain-name

Syntax Description

domain	Specifies the domain name string of the client.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

group (firewall)

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*

no group *id*

Syntax Description

id	Redundancy group ID. Valid values are 1 and 2.

Command Default

No group is configured.

Command Modes

Redundancy application configuration (config-red-app)

Command History

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

Examples

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

hardware-address

To specify the hardware address of a BOOTP client, use the **hardware-address** command in DHCP pool configuration mode. To remove the hardware address, use the no form of this command.

hardware-address *hardware-address* [*protocol-type*| *hardware-number*]

no hardware-address

Syntax Description

hardware-address	MAC address of the client.
protocol-type	(Optional) Protocol type. The valid entries are: • **ethernet** • **ieee802** If no protocol type is specified, the default is Ethernet.
hardware-number	(Optional) ARP hardware specified in an online database at http://www.iana.org/assignments/arp-parameters. The valid range is from 0 to 255. See the table below for valid entries.

Command Default

Only the hardware address is enabled.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid for manual bindings only.

The table below lists the valid assigned hardware numbers found online at http://www.iana.org/assignments/arp-parameters.

Table 1: ARP Hardware Numbers and Types

Hardware Number	Hardware Type
1	Ethernet
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25
4	ProNET Token Ring
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM) (RFC2225)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)
22	MIL-STD-188-220
23	Metricom

Hardware Number	Hardware Type
24	IEEE 1394.1995
25	MAPOS and Common Air Interface (CAI)
26	Twinaxial
27	EUI-64
28	HIPARP
29	IP and ARP over ISO 7816-3
30	ARPSec
31	IPsec tunnel (RFC3456)
32	InfiniBand (RFC-ietf-ipoib-ip-over-infiniband-09.txt)
33	TIA-102 Project

Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
hardware-address b708.1388.f166 ieee802
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a DHCP client in dotted hexadecimal notation.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host**command in DHCP pool configuration mode. To remove the IP address of the client, use the no form of this command.

host *address* [*mask*| /*prefix-length*]

no host

Syntax Description

address	Specifies the IP address of the client.
mask	(Optional) Specifies the network mask of the client.
/ *prefix-length*	(Optional) Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Command Default

The natural mask is used.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the mask and prefix length are unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used. This command is valid for manual bindings only.

There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

Examples

The following example specifies 10.12.1.99 as the IP address of the client and 255.255.248.0 as the subnet mask:

```
host 10.12.1.99 255.255.248.0
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
hardware-address	Specifies the hardware address of a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

host (host-list)

To specify a list of hosts that will receive Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **host**command in host-list configuration mode. To disable the host list, use the **no** form of this command.

host [**vrf** *vrf-name*] {*host-ip-address*| *hostname*}

no host [**vrf** *vrf-name*] {*host-ip-address*| *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) table. The *vrf-name* argument is a name with which the address pool is associated. **Note** All hostnames or IP addresses specified on the same line as the **vrf** keyword are associated with that VRF.
host-ip-address	List of server IP addresses that will receive DDNS updates.
hostname	Specifies a hostname.

Command Default

No list is configured for hosts.

Command Modes

Host-list 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.

Examples

The following example shows how to configure a list of hosts:

```
ip host-list test
 host vrf abc 10.10.0.0
```

Related Commands

Command	Description
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.

Command	Description
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

http (DDNS-update-method)

To specify an update method for address (A) and pointer (PTR) Resource Records (RRs) as HTTP and enter DDNS-HTTP configuration mode, use the **http**command in DDNS-update-method configuration mode. To disable HTTP dynamic updates, use the **no** form of this command.

http {**add** *url-string*| **remove** *url-string*}

no http

Syntax Description

add *url-string*	URL to be used to add or change a mapping between a hostname and an IP address. The *url-string*argumenttakes the following form: http://*userid*:*password*@*domain-name*/*update-folder-name*/**update?system=** *system-name* **&hostname=** *hostname* **&myip=** *myipaddr* • *userid* and *password*--Strings for the organization website that you use for performing the A and PTR RRs updates. • *domain-name* --String for the organizational URL that you are using for the updates; for example www.Cisco.com. • *update-folder-name* --String of the folder name within the organizational website in which your updates are stored. • **update?system** =*system-name* --Update system (method) being used; for example, dydns is DDNS and dyn is EasyDNS. **Note** Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the ? without the software interpreting the ? as a help query. • **&hostname=** *hostname*-- Hostname to update. • **&myip** =*myipaddr*--IP address with which the specified hostname is associated, respectively. **Note** There is one additional special character string, <s>, which could also be entered into the *url-string*. If <s> is entered, when the update is processed, the IP address of the server to which the update is being sent is substituted at that location.

remove *url-string*	URL to be used to remove a mapping between a hostname and an IP address. The *url-string* argument takes the same form as the one shown in the **add** keyword description.

Command Default

No HTTP update method is configured.

Command Modes

DDNS-update-method 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.

Examples

The following example shows how to specify the DynDNS.org to process the updates:

```
ip ddns update method unit-test
 http add http://myuserid:secret@members.dyndns.org/nic/update?system=dyndns&hostname=
mywebsite&myip=10.10.10.10
```

The following are examples of URLs that can be used to update some HTTP DNS update services. These URLs are correct to the best of the knowledge of Cisco but have not been tested in all cases. Where the word “USERNAME:” appears in the URL, your account username at the HTTP site should be used. Where the word “PASSWORD” appears in the URL, your password for that account should be used:

Examples

```
http://USERNAME:PASSWORD@members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
!Requires “interval max 28 0 0 0" in the update method definition.
```

Examples

```
http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>&Email=USERNAME&TZOKey=PASSWORD&IP
Address=<a>
```

Examples

```
http://USERNAME:PASSWORD@members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&
host_id=<h>
```

Examples

```
http://USERNAME:PASSWORD@www.justlinux.com/bin/controlpanel/dyndns/jlc.pl?direst=1&
username=USERNAME&password=PASSWORD&host=<h>&ip=<a>
```

Examples

```
http://USERNAME:PASSWORD@www.dyns.cx/postscript.php?username=USERNAME&password=PASSWORD&
host=<h>&ip=<a>
```

Examples

```
http://USERNAME:PASSWORD@dup.hn.org/vanity/update?ver=1&IP=<a>
```

Examples

```
http://USERNAME:PASSWORD@www.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
```

Note Because these services are provided by the respective companies, the URLs may be subject to change or the service could be discontinued at any time. Cisco takes no responsibility for the accuracy or use of any of this information. The URLs were obtained using an application called "ez-ipupdate," which is available for free on the Internet.

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
default	Specifies the command default.
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
internal	Specifies the internal Cisco IOS cache is used for DDNS updates of A and PTR RRs.
interval maximum	Specifies a maximum interval for DDNS updates of A and PTR RRs.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Enables DDNS as the update method and assigns a method name.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.

Command	Description
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

import all

To import Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP server database, use the **import all** command in DHCP pool configuration mode. To disable this feature, use the **no** form of this command.

import all

no import all

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **no import all** command is used, the DHCP server deletes all "imported" option parameters that were added to the specified pool in the server database. Manually configured DHCP option parameters override imported DHCP option parameters.

Imported option parameters are not part of the router configuration and are not saved in NVRAM.

Examples

The following example allows the importing of all DHCP options for a pool named pool1:

```
ip dhcp pool pool1
 network 172.16.0.0 /16
 import all
```

Related Commands

Command	Description
ip dhcp database	Configures a DHCP server to save automatic bindings on a remote host called a database agent.

Command	Description
show ip dhcp import	Displays the option parameters that were imported into the DHCP server database.

import dns-server

To import the Domain Name System (DNS) recursive name server option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import dns-server**command in IPv6 DHCP pool configuration mode. To remove the available DNS recursive name server list, use the **no** form of this command.

import dns-server

no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name

no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh

no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address

no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nis domain-name

To import the network information service (NIS) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nis domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS domain name is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client.

The NIS domain name option code is 29.

Examples

The following example shows how to import a client's NIS domain name:

```
import nis domain-name
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.

Command	Description
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address

no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name

no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.

Command	Description
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address**command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address

no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import
 sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name**command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name

no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*

no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This 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 SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The SNTP address option can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the SNTP server address:

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*]| **infinity**}

no information refresh {*days* [*hours minutes*]| **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.

internal (DDNS-update-method)

To specify an update method for Dynamic Domain Name System (DDNS) address (A) and pointer (PTR) Resource Records (RRs) as a Cisco IOS internal cache, use the **internal**command in DDNS-update-method configuration mode. To disable the internal dynamic updates, use the **no** form of this command.

internal

no internal

Syntax Description

This command has no arguments or keywords.

Command Default

No internal cache update method is configured.

Command Modes

DDNS-update-method 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is useful in conjunction with turning on the internal Cisco IOS DNS name-server. The DNS name-server is enabled by using the **ip dns server** command. This command enables the name-server to reply to requests for an IP address associated with the hostname that was added to the internal name cache. Not all images have Cisco IOS DNS name-server functionality, so the internal command will not be available. Refer to Feature Navigator at http://www.cisco.com/go/fn to verify the name-server functionality in your image.

When the internal type of update is specified, an entry into the Cisco IOS name cache is added, which is basically the same as entering the **ip host abc.com 10.0.0.1** command. The hostname “abc” and the IP address “10.0.0.1” are associated with an interface.

Examples

The following example shows how to configure a server to send DDNS updates to the internal Cisco IOS cache:

```
ip ddns update method mytest
 internal
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

interval maximum

To specify a maximum interval at which Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) occur, use the **interval maximum**command in DDNS-update-method configuration mode. To disable the interval, use the **no** form of this command.

interval maximum *days hours minutes seconds*

no interval maximum

Syntax Description

days	Maximum interval, in days, at which updates occur. The range is from 0 to 365.
hours	Maximum interval, in hours, at which updates occur. The range is from 0 to 23.
minutes	Maximum interval, in minutes, at which updates occur. The range is from 0 to 59.
seconds	Maximum interval, in seconds, at which updates occur. The range is from 0 to 59.

Command Default

No maximum interval is configured.

Command Modes

DDNS-update-method 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.

Examples

The following example shows how to configure the update method, the maximum interval of the updates (globally), and the hostname on the interface:

```
interface ethernet1
 ip ddns update hostname abc.dyndns.org
 ip ddns update mytest
ip ddns update method mytest
 http add http://test:test@members.dyndns.org/nic/update?system=dyndns&hostname=myhost&
 myip=10.10.10.10
 interval maximum 1 0 0 0
```

Related Commands

Command	Description
ip ddns update method	Enables DDNS as the update method and assigns a method name.

interval minimum

To specify a minimum interval at which Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) occur, use the **interval minimum**command in DDNS-update-method configuration mode. To disable the minimum interval, use the **no** form of this command.

interval minimum *days hours minutes seconds*

no interval minimum

Syntax Description

days	Minimum interval, in days, at which updates occur. The range is from 0 to 365.
hours	Minimum interval, in hours, at which updates occur. The range is from 0 to 23.
minutes	Minimum interval, in minutes, at which updates occur. The range is from 0 to 59.
seconds	Minimum interval, in seconds, at which updates occur. The range is from 0 to 59.

Command Default

No minimum interval is configured.

Command Modes

DDNS-update-method configuration

Usage Guidelines

DDNS updates for interfaces acquiring their address through DHCP occur every time the DHCP lease is renewed. If the lease is renewed more often than the minimum update interval needed, then a problem may occur with the updates. Sites accepting HTTP-style updates, such as DynDNS.org, may report an error if the updates occur too often. The **interval minimum** command forces the system to ignore updates that would occur too often.

Currently, the DynDNS.org policy is that updates can not be made more often than once every 10 minutes. This policy is subject to change in the future. The **interval minimum** command helps to guarantee that updates will not be sent too often.

Command History

Release	Modification
12.4	This command was introduced.

Examples

The following example shows how to configure the minimum interval so that updates would not be sent to DynDNS.org any more often than once every 15 minutes.

```
!
 ip ddns update method my test
 interval minimum 0 0 15 0
 http
 add  http://test:test@members.dyndns.org/nic/update?system=dyndns&hostname=myhostname&
 myip=10.10.10 .1
```

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
http	Specifies HTTP as the update method for A and PTR RRs.
internal	Specifies the internal Cisco IOS cache is used for DDNS udpates of A and PTR RRs.
interval maximum	Specifies a maximum interval at which DDNS updates of A and pointer PTR Resource RRs occur.
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Enables DDNS as the update method and assigns a method name.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.

Command	Description
show ip ddns update method	Displays information about the DDNS update method.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

ip address

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

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

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

Syntax Description

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

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The **vrf** keyword and *vrf-name* argument were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

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

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

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

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

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

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

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

- Disable IP routing (specify the **no ip routing** command).

- Add the interface to a bridge group, see the **bridge-group** command.

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

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autoclassify source
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip address dhcp

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

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id**keyword and *interface-type number*argument were added.
12.2(3)	This command was modified. The **hostname**keyword and *hostname*argument were added. The behavior of the **client-id** *interface-type number*option changed. See the “Usage Guidelines” section for details.

Release	Modification
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelines

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

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

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

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

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

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

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

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

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

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

Table 2: Configuration Method and Resulting Contents of the DISCOVER Message

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

Examples

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

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

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

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

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

```
hostname abc
!
```

```
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

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

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

Related Commands

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

ip address pool (DHCP)

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

ip address pool *name*

no ip address pool

Syntax Description

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

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example specifies that the IP address of Ethernet interface 2 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface Ethernet 2
  ip address pool abc
```

Related Commands

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

ip arp entry learn

To specify the maximum number of learned Address Resolution Protocol (ARP) entries, use the **ip arp entry learn** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip arp entry learn *max-limit*

no ip arp entry learn *max-limit*

Syntax Description

max-limit	The maximum number of learned ARP entries; valid values are from 1 to 512000.

Command Default

No maximum number of learned ARP entries is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD3	This command was introduced to support the Cisco 7600 router.

Usage Guidelines

The **ip arp entry learn** command is available on the Cisco 7600 series routers, which can support a maximum limit of learned ARP entries of 256,000. If a memory card is installed on the router the maximum limit is extended to 512,000.

When the number of ARP entries that can be created by the system is not limited, memory exhaustion can cause system instability. The **ip arp entry learn** command overcomes this problem by defining a maximum number of learned ARP entries.

The limit is not enforced on nonlearned entries. Upon reaching the learn ARP entry threshold limit, or 80 percent of the configured maximum limit, the system will generate a syslog message with a priority set to Level 3 (LOG_NOTICE). Upon reaching the configured maximum limit, the system starts discarding newly learned ARP entries and generates a syslog message. The priority will be set to Level 3 (LOG_NOTICE). The system administrator will have to take appropriate action.

A syslog message is also generated when the number of learned ARP entries in the ARP table decreases from the maximum configured limit to the permit threshold limit, or 95 percent of the maximum configured limit to notify the system administrator that the ARP table is back to normal operation.

The default behavior of the system is not to enforce a maximum limit of learned ARP entries on the system.

When a user tries to configure a maximum limit value for the number of ARP entries that is lower than the current number of ARP entries in the system, the configuration will be rejected with an error message.

The following example configures a maximum limit of the number of learned ARP entries of 512,000:

```
Router# configure terminal
Router(config)# ip arp entry learn 512000
```

Related Commands

Command	Description
show arp summary	Displays the total number of ARP table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router.