Cisco IOS IP Addressing Services Command Reference

December 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS IP Addressing Services Command Reference

CONTENTS

Introduction

This book describes the commands used to configure and monitor IP addressing services. The commands are listed alphabetically within technology area.

For IP addressing services configuration tasks and examples, refer to the *Cisco IOS IP Addressing Services Configuration Guide*.

ARP Commands

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode. To remove an entry from the ARP cache, use the **no** form of this command.

arp {*ip-address* **|** **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*]

no arp {*ip-address* **|** **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*]

Syntax Description

ip-address	IP address in four-part dotted decimal format corresponding to the local data-link address.
vrf *vrf-name*	Virtual Routing and Forwarding (VRF) instance. The *vrf-name* argument is the name of the VRF table.
hardware-address	Local data-link address (a 48-bit address).
encap-type	Encapsulation description. The keywords are as follows: • **arpa**—For Ethernet interfaces. • **sap**—For Hewlett Packard interfaces. • **smds**—For Switched Multimegabit Data Service (SMDS) interfaces. • **snap**—For FDDI and Token Ring interfaces. • **srp-a**—Switch Route Processor, side A (SRP-A) interfaces. • **srp-b**—Switch Route Processor, side B (SRP-B) interfaces.
interface-type	(Optional) Interface type. The keywords are as follows: • **ethernet**—IEEE 802.3 interface. • **loopback**—Loopback interface. • **null**—No interface. • **serial**—Serial interface. • **alias**—Cisco IOS software responds to ARP requests as if it were the interface of the specified address.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 10.31.7.19 0800.0900.1834 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.

arp (interface)

To support a type of encapsulation for a specific network, such as Ethernet, Fiber Distributed Data Interface (FDDI), Frame Relay, and Token Ring, so that the 48-bit Media Access Control (MAC) address can be matched to a corresponding 32-bit IP address for address resolution, use the **arp** command in interface configuration mode. To disable an encapsulation type, use the **no** form of this command.

arp {**arpa** | **frame-relay** | **snap**}

no arp {**arpa** | **frame-relay** | **snap**}

Syntax Description

arpa	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
frame-relay	Enables ARP over a Frame Relay encapsulated interface.
snap	ARP packets conforming to RFC 1042.

Defaults

Standard Ethernet-style ARP

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **probe** keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.
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

Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of encapsulation.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces** EXEC command displays the type of encapsulation being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following example enables Frame Relay services:

```
interface ethernet 0
 arp frame-relay
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp access-list

To configure an Address Resolution Protocol access control list (ARP ACL) for ARP inspection and QoS filtering and enter the ARP ACL configuration submode, use the **arp access-list** command in global configuration mode. To remove the ARP ACL, use the **no** form of this command.

arp access-list *name*

no arp access-list *name*

Syntax Description

name	Name of the access list.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to support DAI on the Supervisor Engine 720. See the “Usage Guidelines” section for the syntax description.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Once you are in the ARP ACL configuration submode, you can add **permit** or **deny** clauses to permit or deny QoS to the flows. The following syntax is available in the ARP QoS ACL configuration submode for QoS filtering; all other configurations will be rejected at the time of the policy-map attachment to the interfaces:

{**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} **mac any**

no {**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} **mac any**

permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.
host *sender-ip*	Specifies the IP address of the host sender.
sender-ip-mask	(Optional) Subnet mask of the host sender.
mac any	Specifies MAC-layer ARP traffic.
no	Deletes an ACE from an ARP ACL.

Once you are in the ARP ACL configuration submode, the following configuration commands are available for ARP inspection:

- **default**—Sets a command to its defaults. You can use the **deny** and **permit** keywords and arguments to configure the default settings.
- **deny**—Specifies the packets to reject.
- **exit**—Exits the ACL configuration mode.
- **no**—Negates a command or set its defaults.
- **permit**— Specifies the packets to forward.

You can enter the **permit** or **deny** keywords to configure the permit or deny clauses to forward or drop ARP packets based on some matching criteria. The syntax for the **permit** and **deny** keywords are as follows:

{**permit** | **deny**} **ip** {**any** | **host** *sender-ip* [*sender-ip sender-ip-mask*]} **mac** {**any** | **host** *sender-mac* [*sender-mac-mask*]} [**log**]

{**permit** | **deny**} **request ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} **mac** {**any** | **host** *sender-mac* [*sender-mac-mask*]} [**log**]

{**permit** | **deny**} **response ip** {**any** | **host** *sender-ip* [*sender-ip-mask*]} [**any** | **host** *target-ip* [*target-ip-mask*]] **mac** {**any** | **host** *sender-mac* [*sender-mac-mask*]} [**any** | **host** *target-mac* [*target-mac-mask*]] [**log**]

permit	Specifies packets to forward.
deny	Specifies packets to reject.
ip	Specifies the sender IP address.
any	Specifies any sender IP address.
host	Specifies a single sender host.
sender-ip	IP address of the host sender.
sender-ip-mask	Subnet mask of the host sender.
mac any	Specifies any MAC address.
mac host	Specifies a single sender host MAC address.
sender-mac	MAC address of the host sender.
sender-mac-mask	Subnet mask of the host sender.
log	(Optional) Specifies log on match.
request	Specifies ARP requests.
response	Specifies ARP responses.
any	(Optional) Specifies any target address.
host	(Optional) Specifies a single target host.
target-ip	IP address of the target host.
target-ip-mask	Subnet mask of the target host.
target-mac	MAC address of the target host.
target-mac-mask	Subnet mask of the target host.

If you enter the **ip** keyword without the **request** or **response** keywords, the configuration applies to both requests and responses.

Once you define an ARP ACL, you can apply it to VLANs using the **ip arp inspection filter** command for ARP inspection.

Incoming ARP packets are compared against the ARP access list, and packets are permitted only if the access list permits them. If access lists deny packets because of explicit denies, they are dropped. If packets get denied because of the implicit deny, they are matched against the list of DHCP bindings, unless the access list is static or the packets are not compared against the bindings.

When a ARP access list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only IP-to-Ethernet MAC bindings are compared against the ACLs. All other type of packets are bridged in the incoming VLAN without any validation.

ACL entries are scanned in the order that you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the ACL.

An implicit **deny ip any mac any** entry exists at the end of an ACL unless you include an explicit **permit ip any mac any** entry at the end of the list.

All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Examples

This example shows how to create a new ARP ACL or enter the submode of an existing ARP ACL:

```
Router(config)# arp access-list arpacl22
Router(config-arp-nacl)#
```

This example shows how to create an ARP ACL named arp_filtering that denies QoS but permits MAC-layer ARP traffic:

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 10.1.1.1 mac any
Router(config-arp-nacl)# deny ip any mac any
Router(config-arp-nacl)#
```

Related Commands

Command	Description
show arp	Displays information about the ARP table.

arp authorized

To disable dynamic Address Resolution Protocol (ARP) learning on an interface, use the **arp authorized** command in interface configuration mode. To reenable dynamic ARP learning, use the **no** form of this command.

arp authorized

no arp authorized

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **arp authorized** command disables dynamic ARP learning on an interface. This command enhances security in public wireless LANs (PWLANs) by limiting the leasing of IP addresses to mobile users and authorized users. The mapping of IP address to MAC address for an interface can be installed only by the authorized subsystem. Unauthorized clients cannot respond to ARP requests.

If both static and authorized ARP are installing the same ARP entry, the static configuration overrides the authorized ARP entry. To install a static ARP entry use the **arp** (global) command. A nondynamic ARP entry can only be removed by using the same method by which it was installed.

The **arp authorized** command can only be specified on Ethernet interfaces and for Dynamic Host Configuration Protocol (DHCP) networks.

Examples

The following example disables dynamic ARP learning on interface Ethernet 0:

```
interface Ethernet0
 ip address 10.0.0.1 255.255.255.0
 arp authorized
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

arp log threshold entries

To enable an Address Resolution Protocol (ARP) trap so that the ARP log is triggered when a specific number of dynamically learned entries is reached on the router interface, use the **arp log threshold entries** command in interface configuration mode. To disable the ARP trap for the interface, use the **no** form of this command.

arp log threshold entries *entry-count*

no arp log threshold entries

Syntax Description

entry-count	Triggers the ARP log service when the number of dynamically learned entries on the interface reaches this threshold. The range is from 1 to 2147483647.

Command Default

ARP trap is disabled for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command enables an ARP trap for the router interface. When the number of dynamically learned entries on the interface exceeds the preconfigured amount, an ARP event message is written to system message logging (syslog) output.

A high number of learned entries on the interface might indicate anomalies such as an attempt to breach security through an ARP attack on the router. The threshold at which to configure the ARP log service trigger should be determined heuristically, based on the expected number of nodes the router will serve and the number of hosts on the interface.

To display information about the setting configured by the **arp log threshold entries** command, use the **show running-config** command. If an ARP trap is enabled for a given interface, the information for that **interface** command includes the **arp log threshold entries** command, followed by the threshold value.

To display the syslog history statistics and buffer contents, use the **show logging** command.

Examples

The following example shows how to enable an ARP trap so that the ARP log is triggered when 50 dynamically learned entries is reached on the Ethernet interface at slot 2, port 1:

```
Router(config)# interface ethernet2/1
Router(config-if)# arp log threshold entries 50
```

The following sample output from the **show logging** command shows that the ARP trap entry was triggered when 50 dynamic ARP entries was reached on the Ethernet interface at slot 2, port 1:

```
Router# show logging

Syslog logging: enabled (0 messages dropped, 39 messages rate-limited, 0 flushes, 0 
overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 309 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.

    Trap logging: level informational, 312 message lines logged

Log Buffer (65536 bytes):

Jan 27 18:27:32.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:27:31 PST 
Fri Jan 27 2006 to 10:27:32 PST Fri Jan 27 2006, configured from console by console.
Jan 27 18:27:32.431: %SYS-5-CONFIG_I: Configured from console by console
Jan 27 18:27:34.051: %ARP-4-TRAPENTRY: 50 dynamic ARP entries on Ethernet2/1 installed in 
the ARP table
```

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
show logging	Displays the contents of logging buffers.
show running-config	Displays the contents of the currently running configuration file of your routing device.

arp packet-priority enable

To enable Address Resolution Protocol (ARP) packet priority on an interface, use the **arp packet-priority enable** command in interface configuration mode. To disable ARP packet priority, use the **no** form of this command.

arp packet-priority enable

no arp packet-priority enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, ARP packet priority is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **arp packet-priority enable** command when a network congestion causes ARP packets to drop. Enabling ARP packet priority significantly reduces the number of ARP packet drops.

Before you configure the **arp packet-priority enable** command, you must configure an IP address for the interface and ensure that the interface is enabled. If the interface is disabled, use the **no shutdown** command to enable the interface.

Examples

The following example shows how to enable packet priority on a Fast Ethernet interface:

```
Router(config)# interface FastEthernet0/1
Router(config-if)# no shutdown
Router(config-if)# ip address 198.51.100.253 255.255.255.0
Router(config-if)# arp packet-priority enable
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
shutdown (interface)	Disables an interface.

arp probe interval

To control the the probing of authorized peers, use the **arp probe interval** command in interface configuration mode. To disable the probe, use the **no** form of this command.

arp probe interval *seconds* **count** *count-number*

no arp probe

Syntax Description

seconds	Interval in seconds after which the next probe will be sent to see if the peer is still present. The range is from 1 to 10.
count *count-number*	Number of probe retries. If no response, the peer has logged off. The range is from 1 to 60.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Once you configure the **arp probe interval** command, probing continues until you disable it using the **no** form of the command on all interfaces.

Examples

The following example shows a 2 second interval with a probe of the peer occurring 5 times:

```
interface ethernet 0
 arp probe interval 2 count 5
```

Related Commands

Command	Description
arp (interface)	Controls the interface-specific handling of IP address resolution.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp timeout

To configure how long a dynamically learned IP address and its corresponding Media Control Access (MAC) address remain in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

seconds	Time (in seconds) that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.

Defaults

14400 seconds (4 hours)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is ignored when issued on interfaces that do not use ARP. The **show interfaces** EXEC command displays the ARP timeout value. The value follows the "Entry Timeout:" heading, as seen in the following example from the **show interfaces** command:

```
ARP type: ARPA, PROBE, Entry Timeout: 14400 sec
```

Examples

The following example sets the ARP timeout to 12000 seconds to allow entries to time out more quickly than the default:

```
interface ethernet 0
 arp timeout 12000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

clear arp-cache

To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the **clear arp-cache** command in privileged EXEC mode.

clear arp-cache [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*]

Syntax Description

interface *type number*	(Optional) Refreshes only the ARP table entries associated with this interface.
vrf *vrf-name*	(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance and the IP address specified by the *ip-address* argument.
ip-address	(Optional) Refreshes only the ARP table entries for the specified IP address.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	The **interface** keyword and the *type* and *number* arguments were made optional to support refreshing of entries for a single router interface. The **vrf** keyword, the *vrf-name* argument, and the *ip-address* argument were added to support refreshing of entries of a specified address and an optionally specified VRF.
12.2(23)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command updates the dynamically learned IP address and MAC address mapping information in the ARP table to ensure the validity of those entries. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), those entries are aged out of the ARP table immediately as opposed to at the next refresh interval.

Note By default, dynamically learned ARP entries remain in the ARP table for four minutes.

The **clear arp-cache** command can be entered multiple times to refresh dynamically created entries from the ARP cache using different selection criteria.

- Use this command without any arguments or keywords to refresh all ARP cache entries for all enabled interfaces.
- To refresh ARP cache entries for a specific interface, use this command with the **interface** keyword and *type* and *number* arguments.

Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, 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 *type* and *number* arguments in the **clear arp-cache interface** command.

- To refresh ARP cache entries from the global VRF and for a specific host, use this command with the *ip-address* argument.
- To refresh ARP cache entries from a named VRF and for a specific host, use this command with the **vrf** keyword and the *vrf-name* and *ip-address* arguments.

To display ARP table entries, use the **show arp** command.

This command does not affect permanent entries in the ARP cache, and it does not affect the ARP HA statistics.

- To remove static ARP entries from the ARP cache, use the **no** form of the **arp** command.
- To remove alias ARP entries from the ARP cache use the **no** form of the **arp** command with the **alias** keyword.
- To reset the ARP HA status and statistics, use the clear arp-cache counters ha command.

Examples

The following example shows how to refresh all dynamically learned ARP cache entries for all enabled interfaces:

```
Router# clear arp-cache
```

The following example shows how to refresh dynamically learned ARP cache entries for the Ethernet interface at slot 1, port 2:

```
Router# clear arp-cache interface ethernet1/2
```

The following example shows how to refresh dynamically learned ARP cache entries for the host at 192.0.2.140:

```
Router# clear arp-cache 192.0.2.140
```

The following example shows how to refresh dynamically learned ARP cache entries from the VRF named vpn3 and for the host at 192.0.2.151:

```
Router# clear arp-cache vrf vpn3 192.0.2.151
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
arp timeout	Configures how long a dynamically learned IP address and its corresponding MAC address remain in the ARP cache.
clear arp-cache counters ha	Resets the ARP HA statistics.
show arp	Displays ARP table entries.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

clear arp-cache counters ha

To reset the Address Resolution Protocol (ARP) high availability (HA) statistics, use the **clear arp-cache counters ha** command in privileged EXEC mode.

clear arp-cache counters ha

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **clear arp-cache counters ha** command to reset all ARP high availability statistics for all enabled interfaces.

To display the ARP HA status and statistics, use the **show arp ha** command.

Note The **clear arp-cache counters ha** command and the **show arp ha** command are available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

Examples

The following example shows how to reset the ARP HA statistics:

```
Router# clear arp-cache counters ha
```

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
show arp ha	Displays the ARP HA status and statistics.

clear arp interface

To clear the entire Address Resolution Protocol (ARP) cache on an interface, use the **clear arp interface** command in privileged or user EXEC mode.

clear arp interface *type number*

Syntax Description

type	Interface type.
number	Interface number.

Defaults

No default behavior or values.

Command Modes

Privileged or User EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear arp interface** command to clean up ARP entries associated with an interface.

Examples

The following example clears the ARP cache from Ethernet interface 0:

```
Router# clear arp interface ethernet 0
```

clear ip arp inspection log

To clear the status of the log buffer, use the **clear ip arp inspection log** command in privileged EXEC mode.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to clear the contents of the log buffer:

```
Router# clear ip arp inspection log
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enter the ARP ACL configuration submode.
show ip arp inspection log	Displays the status of the log buffer.

clear ip arp inspection statistics

To clear the dynamic ARP inspection statistics, use the **clear ip arp inspection statistics** command in privileged EXEC mode.

clear ip arp inspection statistics [**vlan** *vlan-range*]

Syntax Description

vlan *vlan-range*	(Optional) Specifies the VLAN range.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to clear the DAI statistics from VLAN 1:

```
Router# clear ip arp inspection statistics vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enter the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Displays the status of the log buffer.

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.

ip arp gratuitous

To enable the gratuitous Address Resolution Protocol (ARP) control on the router, use the **ip arp gratuitous** command in global configuration mode. To disable the ARP control, use the **no** form of this command.

ip arp gratuitous {**local** | **none**}

no ip arp gratuitous

Syntax Description

local	Accepts only local (same subnet) gratuitous arps.
none	Rejects gratuitous arp control.

Command Default

Gratuitous ARP control is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to enable the gratuitous ARP control to accept only local (same subnet) gratuitous arp control:

```
Router> enable
Router# configure terminal
Router(config)# ip arp gratuitous local
```

Related Commands

Command	Description
show arp	Display the entries in the ARP table.

ip arp incomplete

To rectify the Address Resolution Protocol (ARP) retry parameters, use the **ip arp incomplete** command in global configuration mode. To disable the correction of the retry parameters, use the **no** form of this command.

ip arp incomplete {**entries** *number-of-IP-addresses* **|** **retry** *number-of-times*}

no ip arp incomplete {**entries** | **retry**}

Syntax Description

entries	Limits the number of unresolved addresses.
number-of-IP-addresses	Number of IP addresses to resolve. The range is from 1 to 2147483647.
retry	Limits the number of attempts to resolve an address.
number-of-times	Number of times an ARP Request is sent. The range is from 1 to 2147483647.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host.

Examples

The following example shows how to limit the number of unresolved addresses:

```
Router> enable
Router# configure terminal
Router(config)# ip arp incomplete entries 100
```

Related Commands

Command	Description
show arp	Display the entries in the Address Resolution Protocol (ARP) table.

ip arp inspection filter vlan

To permit ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command in global configuration mode. To disable this application, use the **no** form of this command.

ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

Syntax Description

arp-acl-name	Access control list name.
vlan-range	VLAN number or range; valid values are from 1 to 4094.
static	(Optional) Treats implicit denies in the ARP ACL as explicit denies and drops packets that do not match any previous clauses in the ACL.

Defaults

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

For *vlan-range*, you can specify the VLAN to which the switches and hosts belong. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

If you do not specify the **static** keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

Examples

This example shows how to apply the ARP ACL static-hosts to VLAN 1 for DAI:

```
Router(config)# ip arp inspection filter static-hosts vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection limit (interface configuration)

To limit the rate of incoming ARP requests and responses on an interface and prevent DAI from consuming all of the system's resources in the event of a DoS attack, use the **ip arp inspection limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ip arp inspection limit rate *pps* [**burst interval** *seconds* | **none**]

no ip arp inspection limit

Syntax Description

rate *pps*	Specifies the upper limit on the number of incoming packets processed per second; valid values are from 1 to 2048 pps.
burst interval *seconds*	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets; valid values are from 1 to 15 seconds.
none	(Optional) Specifies that there is no upper limit on the rate of the incoming ARP packets that can be processed.

Defaults

The default settings are as follows:

- The **rate** *pps* is set to **15** packets per second on the untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.
- The rate is unlimited on all the trusted interfaces.
- The **burst interval** *seconds* is set to **1** second.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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

You should configure the trunk ports with higher rates to reflect their aggregation. When the rate of the incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. You can use the error-disable timeout feature to remove the port from the error-disabled state. The rate applies to both the trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs, or use the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets on the channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

After a switch receives more than the configured rate of packets every second consecutively over a period of burst seconds, the interface is placed into an error-disabled state.

Examples

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Router# configur terminal
Router(config)# interface fa6/3
Router(config-if)# ip arp inspection limit rate 25
```

This example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Router# configure terminal
Router(config)# interface fa6/1
Router(config-if)# ip arp inspection limit rate 20 burst interval 5
```

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection log-buffer

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command in global configuration mode. To disable the parameters, use the **no** form of this command.

ip arp inspection log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}

no ip arp inspection log-buffer {**entries** | **logs**}

Syntax Description

entries *number*	Specifies the number of entries from the logging buffer; valid values are from 0 to 1024.
logs *number*	Specifies the number of entries to be logged in an interval; valid values are from 0 to 1024.
interval *seconds*	Specifies the logging rate; valid values are from 0 to 86400 (1 day).

Defaults

The default settings are as follows:

- When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.
- The **entries** *number* is **32**.
- The **logs** *number is* **5** per second.
- The **interval** *seconds is* **1** second.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

A **0** value for the **logs** *number* indicates that the entries should not be logged out of this buffer.

A **0** value for the **interval** *seconds* keyword and argument indicates an immediate log.

You cannot enter a **0** for both the **logs** *number* and the **interval** *seconds* keywords and arguments.

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but are not logged immediately. Registration for these packets occurs in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

Examples

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Router# configure terminal
Router(config)# ip arp inspection log-buffer entries 45
```

This example shows how to configure the logging rate for 10 logs per 3 seconds:

```
Router(config)# ip arp inspection log-buffer logs 10 interval 3
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command in interface configuration mode. To make the interfaces untrusted, use the **no** form of this command.

ip arp inspection trust

no ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to configure an interface to be trusted:

```
Router# configure terminal
Router(config)# interface fastEthernet 6/3
Router(config-if)# ip arp inspection trust
```

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command in global configuration mode. To disable ARP inspection checks, use the **no** form of this command.

ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]

no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]

Syntax Description

src-mac	(Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body.
dst-mac	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
ip	(Optional) Checks the ARP body for invalid and unexpected IP addresses.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

The sender IP addresses are checked in all ARP requests and responses and target IP addresses are checked only in ARP responses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

The **src-mac** checks are issued against both ARP requests and responses. The **dst-mac** checks are issued for ARP responses.

Note When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

The **no** form of this command disables only the specified checks. If no check options are enabled, all the checks are disabled.

Examples

This example shows how to enable the source MAC validation:

```
Router(config)# ip arp inspection validate src-mac
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan

To enable DAI on a per-VLAN basis, use the **ip arp inspection vlan** command in global configuration mode. To disable DAI, use the **no** form of this command.

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

Syntax Description

vlan-range	VLAN number or range; valid values are from 1 to 4094.

Defaults

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

For *vlan-range*, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if the VLAN has not been created or is a private VLAN.

Examples

This example shows how to enable DAI on VLAN 1:

```
Router(config)# ip arp inspection vlan 1
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command in global configuration mode. To disable this logging control, use the **no** form of this command.

ip arp inspection vlan *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**permit** | **all** | **none**}}

no ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **dhcp-bindings**}

Syntax Description

vlan-range	Number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
matchlog	Specifies that logging of packets matched against ACLs is controlled by the **matchlog** keyword in the permit and deny access control entries of the ACL.
none	Specifies that ACL-matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by DHCP bindings.
none	Prevents all logging of packets permitted or denied by DHCP bindings.

Defaults

All denied or dropped packets are logged.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

By default, the **matchlog** keyword is not available on the ACEs. When you enter the **matchlog** keyword, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny.
- **dhcp-bindings**—Logging on DHCP bindings is reset to log on deny.

Examples

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs:

```
Router(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp proxy disable

To globally disable proxy Address Resolution Protocol (ARP), use the **ip arp proxy disable** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

ip arp proxy disable

no ip arp proxy disable

Syntax Description

This command has no arguments or keywords.

Command Default

Proxy ARP is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2 S	This command was introduced.
12.3(11)T	This command was integrated into 12.3(11)T.
12.2 (18)SXE	This command was integrated into 12.2(18)SXE.

Usage Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration. The **default ip arp proxy** command returns proxy ARP to the default behavior, which is enabled.

Examples

The following example disables proxy ARP:

```
ip arp proxy disable
```

The following example enables proxy ARP:

```
no ip arp proxy disable
```

Related Commands

Command	Description
ip proxy-arp	Enables proxy ARP on an interface.

ip gratuitous-arps

To enable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in an address pool if the transmission has been disabled, use the **ip gratuitous-arps** command in global configuration mode. To disable the transmission, use the **no** form of this command.

ip gratuitous-arps [**non-local**]

no ip gratuitous-arps

Syntax Description

non-local	(Optional) Sends gratuitous ARP messages if a client receives an IP address from a non-local address pool. Gratuitous ARP messages for locally originated peer addresses are not sent by default.

Command Default

Gratuitous ARP messages are not sent out when the client receives the address from the local address pool.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2T	The **non-local** keyword was added and the default behavior of the command changed.
12.4(2)T	The name of this command was changed from **no ip gratuitous-arps** to **ip gratuitous-arps**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A Cisco router will send out a gratuitous ARP message out of all interfaces when a client connects and negotiates an address over a PPP connection. However, by default, gratuitous ARP messages are not sent out when the client receives the address from the local address pool. The **ip gratuitous-arps non-local** command option is the default form and is not saved in the running configuration.

Cisco 10000 Series Router

To maximize the performance of the router, disable gratuitous ARP requests using the **no ip gratuitous-arps** command.

Examples

The following example enables the sending of gratuitous ARP messages if the transmission has been disabled:

```
ip gratuitous-arps
```

ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5c)EX	This command was introduced on the Catalyst 6500 series switches.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E on the Catalyst 6500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.

Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

Examples

The following example shows how to enable the local proxy ARP feature:

```
ip local-proxy-arp
```

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command in interface configuration mode. To disable proxy ARP on the interface, use the **no** form of this command.

ip proxy-arp

no ip proxy-arp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration.

Examples

The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
 ip proxy-arp
```

Related Commands

Command	Description
ip arp proxy disable	Globally disables proxy ARP.

ip sticky-arp (global configuration)

To enable sticky ARP, use the **ip sticky-arp** command in global configuration mode. To disable sticky ARP, use the **no** form of this command.

ip sticky-arp

no ip sticky-arp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

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(18)SXF	This command was changed to support all Layer 3 interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In releases prior to Release 12.2(18)SXF, sticky ARP was supported on PVLAN interfaces only.

You can enter the **ip sticky-arp (interface configuration)** command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

Examples

This example shows how to enable sticky ARP:

```
Router(config) ip sticky-arp
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (interface configuration)	Enables sticky ARP on an interface.
show arp	Displays the ARP table.

ip sticky-arp (interface configuration)

To enable sticky ARP on an interface, use the **ip sticky-arp** command in interface configuration mode. To disable sticky ARP on an interface, use the **no** form of this command.

ip sticky-arp [**ignore**]

no ip sticky-arp [**ignore**]

Syntax Description

ignore	(Optional) Overwrites the **ip sticky-arp** (global configuration) command.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	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

You can enter this command on any Layer 3 interface.

You can enter the **ip sticky-arp ignore** command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.

Examples

This example shows how to enable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp ignore
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (global configuration)	Enables sticky ARP.
show arp	Displays the ARP table.

logging server-arp

To enable the sending of Address Resolution Protocol (ARP) requests for syslog server address during system initialization bootup, use the **logging server-arp** command in global configuration mode. To disable the sending of ARP requests for syslog server addresses, use the **no** form of this command.

logging server-arp

no logging server-arp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.3	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(5)B	This command was integrated into Cisco IOS Release 12.3(5)B.

Usage Guidelines

The **logging server-arp** global configuration command allows the sending of ARP requests for syslog server addresses during system initialization bootup.

When this CLI command is configured and saved to the startup configuration file, the system will send an ARP request for remote syslog server address before sending out the first syslog message.

The command should only be used when the remote syslog server is in the same subnet as the system router sending the ARP request.

Note Use this command even if a static ARP has been configured with the remote syslog server address.

Examples

The following example shows how to enable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# logging server-arp
Router(config)# exit
```

The following example shows how to disable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# no logging server-arp
Router(config)# exit
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode.

no ip gratuitous-arps

To disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool, use the **no ip gratuitous-arps** command in global configuration mode.

no ip gratuitous-arps

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

A Cisco router will send out a gratuitous ARP message when a client connects and negotiates an address over a PPP connection. This transmission occurs even when the client receives the address from a local address pool.

Examples

The following example disables gratuitous arp messages from being sent:

```
no ip gratuitous-arps
```

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** command in user EXEC or privileged EXEC mode.

show arp [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the *vrf-name* argument. If this option is specified, it can be followed by any valid combination of the *arp-mode*, *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
arp-mode	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords: • **alias**—Displays only alias ARP entries. An alias ARP entry is a statically configured (permanent) ARP table entry that is associated with a local IP address. This type of entry can be configured or removed using the **arp** (global) command with the **alias** keyword. • **dynamic**—Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host. • **incomplete**—Displays only incomplete ARP entries. An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host. • **interface**—Displaysonly interface ARP entries. An interface ARP entry contains a local IP address and is derived from an interface. • **static**—Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP entry that is associated with an external host. This type of entry can be configured or removed using the **arp** (global) command. **Note** If this option is specified, it can be followed by any valid combination of the *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
ip-address [*mask*]	(Optional) Displays the entries associated with a specific host or network. **Note** If this option is specified, it can be followed by any valid combination of the *interface-type* and *interface-number* arguments and the **detail** keyword.
interface-type *interface-number*	(Optional) Displays the specified entries that are also associated with this router interface. **Note** If this option is specified, it can be followed by the **detail** keyword.
detail	(Optional) Displays the specified entries with mode-specific details and information about subblocks (if any).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
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 the 12.2 SX release.
12.4(11)T	The **vrf** keyword and *vrf-name* argument were added to limit the display to entries under a specific VRF. The **alias**, **dynamic**, **incomplete**, **interface**, and **static** keywords were added to limit the display to entries in a specific ARP mode. The *ip-address* and *mask* arguments were added to limit the display to entries for a specific host or network. The *interface-type* and *interface-number* arguments were added to limit the display to entries for a specific interface. The **detail** keyword was added to display additional details about the entries.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display all entries in the ARP cache, use this command without any arguments or keywords.

Entry Selection Options

You can to limit the scope of the command output by applying various combinations of the following ARP entry selection criteria:

- Entries under a specific VRF
- Entries in a specific ARP mode
- Entries for a specific host or entries for a specific network
- Entries associated with a specific router interface

Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, 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-type* and *interface-number* arguments in the **show arp** command.

Detailed Output Format

To include additional details about each ARP entry displayed, use this command with the **detail** keyword. When this display option is used, the following additional information is included:

- Mode-specific details (such as entry update time)
- Subblocks (if any)

ARP Adjacency Notification

If Cisco Express Forwarding (CEF) is enabled on the router, the router maintains forwarding information (outbound interface and MAC header rewrite) for adjacent nodes. A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). CEF stores the forwarding information in an adjacency database so that Layer 2 addressing information can be inserted into link-layer headers attached to the ARP packets.

- To verify that IPv4 CEF is running, use the **show ip cef** command.
- To verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct, use the **show adjacency** command.

The ARP table information is one of the sources for CEF adjacency. Whenever the ARP subsystem attaches an ARP table entry to an outbound interface with a valid hardware address, the subsystem issues an internal “ARP adjacency” notification. The notification causes an ARP background process to synchronize that ARP entry with CEF adjacency via the adjacency database. If the synchronization succeeds, IP ARP adjacency is said to be “installed”; if the synchronization fails, IP ARP adjacency is said to have been “withdrawn.”

Note Attachment to an outbound interface occurs only for ARP entries in the following modes: alias, dynamic, static, Application Simple, and Application Timer.

To display detailed information about any ARP adjacency notification that may have occurred, use the **show arp** command with the **detail** keyword. You can use this information to supplement the information available through ARP/CEF adjacency debug trace. To enable debug trace for ARP/CEF adjacency interactions, use the **debug arp** command with the **adjacency** keyword.

ARP Cache Administration

To refresh all entries for the specified interface (or all interfaces) or to refresh all entries of the specified address (or all addresses) in the specified VRF table (or in the global VRF table), use the **clear arp-cache** command.

To enable debugging output for ARP transactions, use the **debug arp** command.

Examples

The following is sample output from the **show arp** command with no optional keywords or arguments specified:

```
Router# show arp

Protocol   Address          Age (min)   Hardware Addr    Type    Interface

Internet   192.0.2.112      120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk  4028.5           29          0000.0c01.0e56   SNAP    Ethernet2
Internet   192.0.2.114      105         0000.a710.859b   ARPA    Ethernet3
AppleTalk  4028.9           -           0000.0c02.a03c   SNAP    Ethernet2
Internet   192.0.2.121      42          0000.a710.68cd   ARPA    Ethernet3
Internet   192.0.2.9        -           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk  4036.9           -           0000.3080.6fd4   SNAP    TokenRing0
Internet   192.0.2.9        -           0000.0c01.7bbd   SNAP    Fddi0
```

Table 1 describes the fields shown in the display.

Table 1 show arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • ARPA—For Ethernet interfaces. • SAP—For Hewlett-Packard interfaces. • SMDS—For Switched Multimegabit Data Service (SMDS) interfaces. • SNAP—For FDDI and Token Ring interfaces. • SRP-A—For Switch Route Processor, side A (SRP-A) interfaces. • SRP-B—For Switch Route Processor, side B (SRP-B) interfaces.
Interface	Indicates the interface associated with this network address.

When this command is used to display dynamic ARP entries, the display information includes the time of the last update and the amount of time before the next scheduled refresh is to occur. The following is sample output from the **show arp** command for the dynamic ARP entry at network address 192.0.2.1:

```
Router# show arp 192.0.2.1 detail

ARP entry for 192.0.2.1, link type IP.
  Alias, last updated 13323 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is complete, attached to GigabitEthernet1/1.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.1 on GigabitEthernet1/1) was installed.
```

When this command is used to display floating static ARP entries, the display information includes the associated interface, if any.The following is sample output from the **show arp** command for the floating static ARP entry at network address 192.0.2.2 whose intended interface is down:

```
Router# show arp 192.0.2.2 detail

ARP entry for 192.0.2.2, link type IP.
  Alias, last updated 13327 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
```

```
  * Static ARP Subblock
    Floating entry.
    Entry is incomplete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.2 on GigabitEthernet1/1) was withdrawn.
```

The following is sample detailed output from the **show arp** command for the Application Alias ARP entry at network address 192.0.2.3:

```
Router# show arp 192.0.2.3 detail

ARP entry for 192.0.2.3, link type IP.
  Application Alias, via Ethernet2/2, last updated 0 minute ago.
  Created by "HSRP".
  Encap type is ARPA, hardware address is 0000.0c07.ac02, 6 bytes long.
  ARP subblocks:
  * Application Alias ARP Subblock
  * HSRP
    ARP Application entry for application HSRP.
```

The following is sample detailed output from the **show arp** command for all dynamic ARP entries:

```
Router# show arp dynamic detail

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1, last updated 0 minute ago.
  Encap type is ARPA, hardware address is 0000.0000.0014, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 0 minute and 1 second.
    It has 1 chance to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
debug arp	Enables debugging output for ARP packet transactions.
show adjacency	Verifies that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip cef	Display entries in the FIB or to display a summary of the FIB.

show arp application

To display Address Resolution Protocol (ARP) table information for a specific ARP application or for all applications supported by ARP and running on registered clients, use the **show arp application** command in user EXEC or privileged EXEC mode.

show arp application [*application-id*] [**detail**]

Syntax Description

application-id	(Optional) Displays ARP table information for a specific ARP application. The range is from 200 to 4294967295. If no ID is specified, ARP table information is displayed for all supported ARP applications running on registered clients.
detail	(Optional) Includes detailed information about subblocks for ARP table information displayed (for the specified application or for all applications supported by ARP and running on registered clients).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display ARP table information about all supported ARP applications running on registered clients, use this command without any arguments or keywords.

Entry Selection Options

To display ARP table information about a single ARP application running on a registered client, use this command with the *application-ID* argument.

Detailed Output Format

To display the specified ARP table information along with detailed information about any subblocks, use this command with the **detail** keyword. The additional details consist of the following information:

- IP address or network
- ARP table entry type (dynamic, interface, static, or alias) or ARP application mode (Simple Application or Application Alias)
- Associated interface
- Brief description of the subblock data

Examples

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

```
Router# show arp application

Number of clients registered: 7

Application         ID        Num of Subblocks
ARP Backup          200       1
IP SIP              201       0
LEC                 202       0
DHCPD               203       0
IP Mobility         204       0
HSRP                209       1
IP ARP Adjacency    212       2
```

The following is sample detailed output from the **show arp application detail** command:

```
Router# show arp application detail

Number of clients registered: 7

Application         ID        Num of Subblocks
ARP Backup          200       1

ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    Backup for Interface on Ethernet2/2

Application         ID        Num of Subblocks
IP SIP              201       0

Application         ID        Num of Subblocks
LEC                 202       0

Application         ID        Num of Subblocks
DHCPD               203       0

Application         ID        Num of Subblocks
IP Mobility         204       0

Application         ID        Num of Subblocks
HSRP                209       1

ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    ARP Application entry for application HSRP.

Application         ID        Num of Subblocks
IP ARP Adjacency    212       2

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
ARP entry for 192.0.2.2, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.2 on Ethernet2/1) was installed.
```

Table 2 describes the significant fields shown in the display.

Table 2 show arp application Field Descriptions

Field	Description
Application	ARP application name
ID	ARP application ID number
Num of Subblocks	Number of subblocks attached

Related Commands

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp ha

To display the status and statistics of Address Resolution Protocol (ARP) high availability (HA), use the **show arp ha** command in user EXEC or privileged EXEC mode.

show arp ha

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display the ARP HA status and statistics.

HA-Capable Platforms

This command is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

ARP HA Statistics

The ARP HA process collects one set of statistics for the active RP (described in Table 3) and a different set of statistics for the standby RP (described in Table 4). These statistics can be used to track the RP state transitions when debugging ARP HA issues.

The output from this command depends on the current and most recent states of the RP:

- For the active RP that has been the active RP since the last time the router was rebooted, this command displays the HA statistics for the active RP.
- For the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred, this command displays the HA statistics for the active RP plus the HA statistics collected when the RP was a standby RP.
- For a standby RP, this command displays the HA statistics for a standby RP.

Examples

The following is sample output from the **show arp ha** command on the active RP that has been the active RP since the last time the router was rebooted. ARP HA statistics are displayed for the active state only.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  2 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  806 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
```

The following is sample output from the **show arp ha** command on the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred. ARP HA statistics are displayed for the active state and also for the previous standby state.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP).
  1 ARP entry in the synchronization queue.
  1 ARP entry waiting to be synchronized.
  No synchronization packet sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.

Statistics collected when ARP HA in standby state:
  No ARP entry in the backup table.
  808 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  2 ARP entries restored before timer.
  No ARP entry restored on timer.
  No ARP entry purged since interface is down.
  No ARP entry purged on timer.
```

The following is sample output from the **show arp ha** command on the standby RP. ARP HA statistics are displayed for the standby state only.

```
Router# show arp ha

ARP HA in standby state (ARP_HA_ST_S_UP).
  2 ARP entries in the backup table.
  806 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

Table 3 describes the significant fields shown in the display collected for an active RP.

Table 3 show arp ha Field Descriptions for Statistics Collected for an Active RP

Field	Description
ARP HA in active state	The current state that the event-driven state machine contains for the active RP: • ARP_HA_ST_A_UP_SYNC—Active state in which the active RP sends entries from the synchronization queue to the standby RP. The active RP transitions into this state when the number of entries to be synchronized reaches a threshold or when the synchronization timer expires, whichever occurs first. • ARP_HA_ST_A_UP—Active state in which the active RP does not send entries to the standby RP. The active RP transitions into this state either because the standby RP has not come up yet or because a previous synchronization has failed. • ARP_HA_ST_A_BULK—Transient state in which the active RP waits for the standby RP to signal that it has finished processing of the entries sent by the bulk-synchronization operation. • ARP_HA_ST_A_SSO—Transient state in which the new active RP waits for the signal to be fully operational.
ARP entries in the synchronization queue	Number of ARP entries that are queued to be synchronized or have already been synchronized to the standby RP. **Note** Entries that have already been synchronized are kept in the synchronization queue in case the standby RP crashes. After the standby RP reboots, the entire queue (including entries that were already synchronized to the standby RP before the crash) must be bulk-synchronized to the standby RP.
ARP entries waiting to be synchronized	Number of ARP entries that are queued to be synchronized to the standby RP.
synchronization packets sent	Number of synchronization packets that have been sent to the standby RP.
error in allocating synchronization packets	Number of errors that occurred while synchronization packets were being allocated.
error in sending synchronization packets.	Number of errors that occurred while synchronization packets were being sent to the standby RP.
error in encoding interface names	Number of errors that occurred while interface names were being encoded.

Table 4 describes the significant fields shown in the display collected for a standby RP or for an active RP that was previously in the active state.

Table 4 show arp ha Field Descriptions for Statistics Collected for a Standby RP

Field	Description
ARP HA in standby state	The current state that the event-driven state machine contains for the standby RP: • ARP_HA_ST_S_BULK—Transient state in which the standby RP processes the entries sent by the bulk-synchronization operation. After the active RP signals that it has finished sending entries, the standby RP transitions into the ARP_HA_ST_S_UP state and then signals back to the active RP that it has finished processing the entries sent by the bulk-synchronization operation. • ARP_HA_ST_S_UP—Active state in which the standby RP processes the incremental ARP synchronization entries from the active RP. When the switchover occurs, the standby RP transitions to the ARP_HA_ST_A_SSO state.
ARP entries in the backup table	Number of ARP entries contained in the backup ARP table.
synchronization packets processed	Number of synchronization packets that were processed.
synchronization packet dropped in invalid state	Number of synchronization packets that were dropped due to an invalid state.
error in decoding interface names	Number of errors that occurred in decoding interface names.
ARP entries restored before timer	Number of ARP entries that the new active RP restored prior to expiration of the “flush” timer.
ARP entry restored on timer	Number of ARP entries that the new active RP restored upon expiration of the “flush” timer.
ARP entry purged since interface is down	Number of ARP entries that the new active RP purged because the interface went down.
ARP entry purged on timer	Number of ARP entries that the new active RP purged upon expiration of the “flush” timer.

Related Commands

Command	Description
clear arp-cache counters ha	Resets the ARP HA statistics.
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp summary

To display the total number of Address Resolution Protocol (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, use the **show arp summary** command in user EXEC or privileged EXEC mode.

show arp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRD3	This command was modified. Support was added for the Cisco 7600 router.

Usage Guidelines

Use this command to display high-level statistics about the ARP table entries:

- Total number of ARP table entries
- Number of ARP table entries for each ARP mode
- Number of ARP table entries for each router interface

A maximum limit for learned ARP entries can be configured on the Cisco 7600 platform in Cisco IOS Release 12.2(33)SRD3. This is subject to memory constraints. The 7600 can support a maximum limit of 256,000 learned ARP entries, and if a memory card is installed on the router the maximum limit is extended to 512,000.

Examples

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

Note In this example the maximum limit for the number of learned ARP entries has not been configured.

```
Router# show arp summary

Total number of entries in the ARP table: 10.
Total number of Dynamic ARP entries: 4.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 4.
Total number of Static ARP entries: 2.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
```

```
Interface Entry Count
Ethernet3/2 1
```

The following is sample output from the **show arp summary** command on a Cisco 7600 router for Cisco IOS Release 12.2(33)SRD3, after a maximum limit is set for the number of learned ARP entries:

```
Router> enable
Router# configure terminal
Router(config)# ip arp entry learn 512000
Router(config)# exit
Router# show arp summary

Total number of entries in the ARP table: 4.
Total number of Dynamic ARP entries: 0.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 3.
Total number of Static ARP entries: 1.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Maximum limit of Learn ARP entry : 512000.
Maximum configured Learn ARP entry limit : 512000.
Learn ARP Entry Threshold is 409600 and Permit Threshold is 486400.
Total number of Learn ARP entries: 0.
Interface              Entry Count
GigabitEthernet4/7               1
GigabitEthernet4/1.1             1
GigabitEthernet4/1               1
EOBC0/0
```

Table 5describes the fields shown in the display.

Table 5 show arp summary Command Field Descriptions

Field	Description
Total Number of entries in the ARP table	Displays the number of entries in the ARP table.
Total number of Dynamic ARP entries	Displays the number of ARP entries in the dynamic state.
Total number of Incomplete ARP entries	Displays the number of ARP entries in the incomplete state.
Total number of Interface ARP entries	Displays the number of ARP entries on ARP enabled interfaces.
Total number of Static ARP entries	Displays the number of active statically configured ARP entries.
Total number of Alias ARP entries	Displays the number of active statically configured alias entries.
Total number of Simple Application ARP entries	Displays the number of ARP entries in the simple application mode.
Total number of Application Alias ARP entries	Displays the number of ARP entries in the application alias mode.
Total number of Application Timer ARP entries	Displays the number of ARP entries in the application timer mode.

Table 5 show arp summary Command Field Descriptions (continued)

Field	Description
Maximum limit of Learn ARP entry	Displays the allowed maximum limit for the learned ARP entries.
Maximum configured Learn ARP entry limit	Displays the figure the maximum learned ARP entry limit is set to.
Learn ARP Entry Threshold	Displays the value representing 80 percent of the set maximum learned ARP entry limit.
Permit Threshold	Displays the value representing 95 percent of the set maximum learned ARP entry limit.
Total number of Learn ARP entries	Displays the total number of learned ARP entries.
Interface	Lists the names of the ARP enabled interfaces.
Entry Count	Displays the number of ARP entries on each ARP enabled interface

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
ip arp entry learn	Specifies the maximum number of learned ARP entries.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

show ip arp [*ip-address*] [*host-name*] [*mac-address*] [*interface type number*]

Syntax Description

ip-address	(Optional) ARP entries matching this IP address are displayed.
host-name	(Optional) Host name.
mac-address	(Optional) 48-bit MAC address.
interface type number	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes

EXEC

Command History

Release	Modification
9.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples

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

```
Router# show ip arp

Protocol  Address             Age(min)       Hardware Addr     Type      Interface
Internet  172.16.233.229      -              0000.0c59.f892    ARPA      Ethernet0/0
Internet  172.16.233.218      -              0000.0c07.ac00    ARPA      Ethernet0/0
Internet  172.16.233.19       -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.233.309      -              0000.0c36.6965    ARPA      Ethernet0/0
Internet  172.16.168.11       -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.168.254      9              0000.0c36.6965    ARPA      Ethernet0/0
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.

Table 6 show ip arp Field Descriptions (continued)

Field	Description
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: • ARPA • SNAP • SAP
Interface	Indicates the interface associated with this network address.

show ip arp inspection

To display the status of DAI for a specific range of VLANs, use the **show ip arp inspection** command in privileged EXEC mode.

show ip arp inspection [**interfaces** [*interface-name*] | **statistics** [**vlan** *vlan-range*]]

Syntax Description

interfaces *interface-name*	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface.
statistics	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
vlan *vlan-range*	(Optional) Displays the statistics for the selected range of VLANs.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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

If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed.

If you do not specify the interface name, the trust state and rate limit for all applicable interfaces in the system are displayed.

Examples

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Router# show ip arp inspection statistics vlan 3

 Vlan      Forwarded         Dropped     DHCP Drops     ACL Drops
 ----      ---------         -------     ----------     ----------
    3          31753          102407         102407              0

 Vlan   DHCP Permits     ACL Permits   Source MAC Failures
 ----   ------------     -----------   -------------------
    3          31753               0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    3                   0                         0
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Router# show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0
    2              0              0              0              0
    3          68322         220356         220356              0
    4              0              0              0              0
  100              0              0              0              0
  101              0              0              0              0
 1006              0              0              0              0
 1007              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0
    2              0              0                     0
    3          68322              0                     0
    4              0              0                     0
  100              0              0                     0
  101              0              0                     0
 1006              0              0                     0
 1007              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
    2                  0                        0
    3                  0                        0
    4                  0                        0
  100                  0                        0
  101                  0                        0
 1006                  0                        0
 1007                  0                        0
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Router# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
```

This example shows how to display the trust state of Fast Ethernet interface 6/3:

```
Router# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa6/1            Untrusted               20                 5
```

This example shows how to display the trust state of the interfaces on the switch:

```
Router# show ip arp inspection interfaces

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted               15
 Gi1/2            Untrusted               15
 Gi3/1            Untrusted               15
 Gi3/2            Untrusted               15
 Fa3/3            Trusted               None
 Fa3/4            Untrusted               15
 Fa3/5            Untrusted               15
 Fa3/6            Untrusted               15
 Fa3/7            Untrusted               15
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

show ip arp inspection log

To show the status of the log buffer, use the **show ip arp inspection log** command in privileged EXEC mode.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Router# show ip arp inspection log

Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.

 Interface        Vlan   Sender MAC         Sender IP        Num of Pkts
 ---------------  -----  -----------------  ---------------  -----------
Fa6/3            1     0002.0002.0002  10.1.1.2         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.3         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.4         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.5         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.6         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.7         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.8         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.9         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.10        1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.11        1(12:02:52 UTC Fri Apr 25 2003)
    --            --         --               --       5(12:02:52 UTC Fri Apr 25 2003)
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Router# clear ip arp inspection log
Router# show ip arp inspection log

Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
```

Related Commands

Command	Description
clear ip arp inspection log	Clear the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

update arp

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

update arp

no update arp

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

This command can be configured only under the following conditions:

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

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

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

Examples

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

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

Related Commands

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

DHCP Commands

accounting (DHCP)

To enable Dynamic Host Configuration Protocol (DHCP) accounting, use the **accounting** command in DHCP pool configuration mode. To disable DHCP accounting for the specified server group, use the **no** form of this command.

accounting *server-group-name*

no accounting *server-group-name*

Syntax Description

server-group-name	Name of a server group to apply DHCP accounting. • The server group can have one or more members. The server group is defined in the configuration of the **aaa group server** and **aaa accounting** commands.

Defaults

DHCP accounting is not enabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The **accounting** command is used to enable the DHCP accounting feature by sending secure DHCP START accounting messages when IP addresses are assigned to DHCP clients, and secure DHCP STOP accounting messages when DHCP leases are terminated. A DHCP lease is terminated when the client explicitly releases the lease, when the session times out, and when the DHCP bindings are cleared from the DHCP database. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

The **accounting** command can be used only to network pools in which bindings are created automatically and destroyed upon lease termination (or when the client sends a DHCP RELEASE message). DHCP bindings are also destroyed when the **clear ip dhcp binding** or **no service dhcp** command is issued. These commands should be used with caution if an address pool is configured with DHCP accounting.

Authentication, authorization, and accounting (AAA) and RADIUS must be configured before this command can be used to enable DHCP accounting. A server group must be defined with the **aaa group server** command. START and STOP message generation is configured with the **aaa accounting** command. The **aaa accounting** command can be configured to enable the DHCP accounting to send both START and STOP messages or STOP messages only.

Examples

The following example shows how to configure DHCP accounting start and stop messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. Stop messages will be sent only if RADIUS-GROUP1 is configured as a stop-only group.

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# accounting group1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
aaa session-id	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that Cisco IOS will look for RADIUS server hosts.
service dhcp	Enables the Cisco IOS DHCP server and relay agent features.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.
update arp	Secures the MAC address of the authorized client interface to the DHCP binding.

address client-id

To reserve an IP address for a Dynamic Host Configuration Protocol (DHCP) client identified by a client identifier, use the **address client-id** command in DHCP pool configuration mode. To remove the reserved address, use the **no** form of this command.

address *ip-address* **client-id** *string* [**ascii**]

no address *ip-address*

Syntax Description

ip-address	IP address reserved for the client.
string	A unique ASCII string or hexadecimal string.
ascii	(Optional) Specifies that the client ID is in ASCII string form.

Command Default

IP addresses are not reserved.

Command Modes

DCHP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The **address client-id** command can be used to create reserved addresses in pools for any DHCP client identified by the client identifier option in the DHCP packet. You can also reserve an IP address for a DHCP client that is configured to use the port-based address allocation feature. For port-based address allocation, the *string* argument must be the short name of the interface (port) and the **ascii** keyword must be specified.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
address hardware address	Reserves an IP address for a client identified by hardware address.

address hardware-address

To reserve an IP address for a client identified by hardware address, use the **address hardware-address** command in DHCP pool configuration mode. To remove the reserved address, use the **no** form of this command.

address *ip-address* **hardware-address** *mac-address* [*hardware-number*]

no address *ip-address*

Syntax Description

ip-address	IP address reserved for the client.
mac-address	Hardware address of the client.
hardware-number	(Optional) Address Resolution Protocol (ARP) hardware specified in an online database at http://www.iana.org/assignments/arp-parameters. The range is from 0 to 255.

Command Default

IP addresses are not reserved.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

This command is used to reserve an IP address for clients identified by the hardware address included in the fixed-size header of the Dynamic Host Configuration Protocol (DHCP) message.

Examples

In the following example, an IP address is reserved for a client that is identified by its hardware address:

```
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# address 10.10.10.3 hardware-address b708.1388.f166
```

Related Commands

Command	Description
address client-id	Reserves an IP address for a DHCP client identified by the client identifier.

address range

To set an address range for a Dynamic Host Configuration Protocol (DHCP) class in a DHCP server address pool, use the **address range** command in DHCP pool class configuration mode. To remove the address range, use the **no** form of this command.

address range *start-ip end-ip*

no address range *start-ip end-ip*

Syntax Description

start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.

Defaults

No default behavior or values

Command Modes

DHCP pool class configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If this command is not configured for a DHCP class in a DHCP server address pool, the default value is the entire subnet of the address pool.

Examples

The following example sets the available address range for class 1 from 10.0.20.1 through 10.0.20.100:

```
ip dhcp pool ABC
 network 10.0.20.0 255.255.255.0
 class CLASS1
 address range 10.0.20.1 10.0.20.100
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

authorization method (DHCP)

To specify a method list to be used for address allocation using RADIUS for Dynamic Host Control Protocol (DHCP), use the **authorization method** command in DHCP pool configuration mode. To disable the authorization method list, use the **no** form of this command.

authorization method *method-list-name*

no authorization method *method-list-name*

Syntax Description

method-list-name	An authorization method list of the network type to be used for this DHCP pool.

Command Default

The authorization network default method list is used for authorization.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The method list must be defined during initial authentication setup.

Examples

The following example shows how to set an authorization method of auth1 to download DHCP information from DHCP or a RADIUS server for DHCP clients when pool_common is used:

```
Router(config)# aaa authorization network auth1 group radius
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.
authorization username (dhcp)	Specifies the parameters that RADIUS sends to a DHCP server when downloading information for a DHCP client.
authorization shared-password	Specifies the password that RADIUS sends to a DHCP or RADIUS server when downloading configuration information for a DHCP client.

authorization shared-password

To specify the password that RADIUS sends to a Dynamic Host Control Protocol (DHCP) or RADIUS server when downloading configuration information for a DHCP client, use the **authorization shared-password** command in DHCP pool configuration mode. To remove the password used for downloading DHCP client configuration, use the **no** form of this command.

authorization shared-password *password*

no authorization shared-password *password*

Syntax Description

password	The password configured in the RADIUS user profile.

Command Default

No password is sent in the RADIUS requests.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is used to enter the password that matches the password configured in a RADIUS user profile, at a RADIUS server, for the username matching the string.

Examples

The following example shows how to set the password to cisco:

```
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.
authorization method (dhcp)	Specifies the method list to be used for address allocation information.
authorization username (dhcp)	Specifies the parameters that RADIUS sends to a DHCP server when downloading information for a DHCP client.

authorization username (DHCP)

To specify the parameters that RADIUS sends to a Dynamic Host Control Protocol (DHCP) server when downloading configuration information for a DHCP client, use the **authorization username** command in DHCP pool configuration mode. To disable the parameters, use the **no** form of this command.

authorization username *string*

no authorization username *string*

Syntax Description

string	A string that RADIUS sends to the DHCP server when downloading an IP address and other configuration information for a client's DHCP responses. The string must contain the following formatting characters to insert information associated with the DHCP client: • **%%**—Transmits the percent sign (%) character in the string sent to the RADIUS server • **%c**—Ethernet address of the DHCP client (chaddr field) in ASCII format • **%C**—Ethernet address of the DHCP client in hexadecimal format • **%g**—Gateway address of the DHCP relay agent (giaddr field) • **%i**—Inner VLAN ID from the DHCP relay information (option 82) in ASCII format • **%I**—Inner VLAN ID from the DHCP relay information in hexadecimal format • **%o**—Outer VLAN ID from the DHCP relay information (option 82) in ASCII format • **%O**—Outer VLAN ID from the DHCP relay information (option 82) in hexadecimal format • **%p**—Port number from the DHCP relay information (option 82) in ASCII format • **%P**—Port number from the DHCP relay information (option 82) in hexadecimal format • **%u**—Circuit ID from the DHCP relay information in ASCII format • **%U**—Circuit ID from the DHCP relay information in hexadecimal format • **%r**—Remote ID from the DHCP relay information in ASCII format • **%R**—Remote ID from the DHCP relay information in hexadecimal format **Note** The percent (%) is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% character.

Command Default

No parameters are specified.

Command Modes

DHCP pool configuration (config-dhcp)

Command History

Release	Modification
12.2(31)ZV1	This command was modified for the DHCP server RADIUS proxy feature on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)ZV1.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

When a DHCP server sends an access request to the authentication, authorization, and accounting (AAA) server, the **%** and character specified in the username are format characters that is replaced by one of the following values based on the characters specified:

- Hardware address
- Inner VLAN ID
- Outer VLAN ID
- Port number
- Circuit ID
- Remote ID

The **%** and character specified in the **authorization username** command configure the DHCP server to send the username in ASCII format or the hexadecimal format based on the case (uppercase or lowercase) of the character used.

For example, if you specify **%C** with the **authorization username** command and the hardware address of the client is aabb.ccdd.eeff, then the DHCP server sends the username as "dhcp-AABBCCDDEEFF" in ASCII format. If you specify **%c** with the **authorization username** command, then the DHCP server sends the username as "646863702daabbccddeeff" in hexadecimal format. The server sends 11 bytes of data when the format is hexadecimal and 19 bytes when the format is ASCII.

Examples

The following example shows how to configure RADIUS to send the Ethernet address of the DHCP client (chaddr field) to the DHCP server when downloading configuration information for a DHCP client:

```
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

Command	Description
authorization method (dhcp)	Specifies the method list to be used for address allocation information.
authorization shared-password	Specifies the password that RADIUS sends to a DHCP or RADIUS server when downloading configuration information for a DHCP client.

bootfile

To specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client, use the **bootfile** command in DHCP pool configuration mode. To delete the boot image name, use the **no** form of this command.

bootfile *filename*

no bootfile

Syntax Description

filename	Specifies the name of the file that is used as a boot image.

Defaults

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 xllboot as the name of the boot file:

```
bootfile xllboot
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
next-server	Configures the next server in the boot process of a DHCP client.

class (DHCP)

To associate a class with a Dynamic Host Configuration Protocol (DHCP) address pool and enter DHCP pool class configuration mode, use the **class** command in DHCP pool configuration mode. To remove the class association, use the **no** form of this command.

class *class-name*

no class *class-name*

Syntax Description

class-name	Name of the DHCP class.

Command Default

No class is associated with the DHCP address pool.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

You must first define the class using the **ip dhcp class** command available in global configuration command. If a nonexistent class is named by the **class** command, the class will be automatically created. Each class in the DHCP pool will be examined for a match in the order configured.

Examples

The following example shows how to associate DHCP class 1 and class 2 with a DHCP pool named pool1:

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# network 10.0.20.0 255.255.255.0
Router(dhcp-config)# class class1
Router(config-dhcp-pool-class)# address range 10.0.20.1 10.0.20.100
Router(config-dhcp-pool-class)# exit
Router(dhcp-config)# class class2
Router(config-dhcp-pool-class)# address range 10.0.20.101 10.0.20.200
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

clear ip dhcp binding

To delete an automatic address binding from the Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** command in privileged EXEC mode.

clear ip dhcp [**pool** *name*] **binding** [**vrf** *vrf-name*] {***** | *address*}

Syntax Description

pool *name*	(Optional) Specifies the name of the DHCP pool.
vrf	(Optional) Clears virtual routing and forwarding (VRF) information from the DHCP database.
vrf-name	(Optional) The VRF name.
*****	Clears all automatic bindings.
address	The address of the binding you want to clear.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	This command was modified. The **pool** keyword and *name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Typically, the address denotes the IP address of the client. If the asterisk (*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp binding** command in global configuration mode to delete a manual binding.

Note the following behavior for the **clear ip dhcp binding** command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the nonvirtual VRF DHCP pools for the specified binding.
- If you do not specify the **pool** *name* option and the ***** option is specified, it is assumed that all automatic or on-demand bindings in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the ***** option, all automatic or on-demand bindings in the specified pool only will be cleared.
- If you specify the **pool** *name* option and an IP address, the specified binding will be deleted from the specified pool.

Examples

The following example shows how to delete the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

The following example shows how to delete all bindings from all pools:

```
Router# clear ip dhcp binding *
```

The following example shows how to delete all bindings from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 binding *
```

The following example shows how to delete address binding 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 binding 10.13.2.99
```

The following example shows how to delete VRF vrf1 from the DHCP database:

```
Router# clear ip dhcp binding vrf vrf1 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

clear ip dhcp conflict

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

clear ip dhcp [**pool** *name*] **conflict** [**vrf** *vrf-name*] {***** | *address*}

Syntax Description

pool *name*	(Optional) Specifies the name of the DHCP pool.
vrf	(Optional) Clears DHCP virtual routing and forwarding (VRF) conflicts.
vrf-name	(Optional) The VRF name.
*****	Clears all address conflicts.
address	The IP address of the host that contains the conflicting address you want to clear.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	This command was modified. The **pool** keyword and *name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The server detects conflicts using a ping operation. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (*) character is used as the address parameter, DHCP clears all conflicts.

Note the following behavior for the **clear ip dhcp conflict** command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the nonvirtual VRF DHCP pools for the specified conflict.
- If you do not specify the **pool** *name* option and the ***** option is specified, it is assumed that all automatic/ or on-demand conflicts in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the ***** option, all automatic or on-demand conflicts in the specified pool only will be cleared.
- If you specify the **pool** *name* option and an IP address, the specified conflict will be deleted from the specified pool.

Examples

The following example shows how to delete an address conflict of 10.12.1.99 from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

The following example shows how to delete all address conflicts from all pools:

```
Router# clear ip dhcp conflict *
```

The following example shows how to delete all address conflicts from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 conflict *
```

The following example shows how to delete address conflict 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 conflict 10.13.2.99
```

The following example shows how to delete VRF vrf1 from the DHCP database:

```
Router# clear ip dhcp conflict vrf vrf1 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

clear ip dhcp limit lease

To clear lease limit violation entries, use the **clear ip dhcp limit lease** command in privileged EXEC mode.

clear ip dhcp limit lease [*interface-type interface-number*]

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ip dhcp limit lease** command displays the number of lease limit violations. You can control the number of subscribers at the global level by using the **ip dhcp limit lease per interface** command and at the interface level by using the **ip dhcp limit lease** command.

Examples

In the following example, the number of lease violations is displayed and then cleared:

```
Router# show ip dhcp limit lease

Interface         Count
Serial0/0.1       5
Serial1           3

Router# clear ip dhcp limit lease

Router# show ip dhcp limit lease
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

clear ip dhcp server statistics

To reset all Dynamic Host Configuration Protocol (DHCP) server counters, use the **clear ip dhcp server statistics** command in privileged EXEC mode.

clear ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

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 **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters will be initialized, or set to zero, with the **clear ip dhcp server statistics** command.

Examples

The following example resets all DHCP counters to zero:

```
Router# clear ip dhcp server statistics
```

Related Commands

Command	Description
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.

clear ip dhcp snooping binding

To clear the DHCP-snooping binding-entry table without disabling DHCP snooping, use the **clear ip dhcp snooping binding** command in privileged EXEC mode.

clear ip dhcp snooping binding

Syntax Description

This command has no arguments or keywords.

Defaults

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 DHCP-snooping binding-entry table:

```
Router# clear ip dhcp snooping binding
```

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

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

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

clear ip dhcp snooping statistics

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

clear ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.

Examples

This example shows how to clear the DHCP snooping statistics:

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

clear ip dhcp subnet

To clear all currently leased subnets in the Dynamic Host Configuration Protocol (DHCP) pool, use the **clear ip dhcp subnet** command in privileged EXEC configuration mode.

clear ip dhcp [**pool** *name*] **subnet** { ***** | *address*}

Syntax Description

pool *name*	(Optional) Name of the DHCP pool.
*****	Clears all leased subnets.
address	Clears a subnet containing the specified IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

A PPP session that is allocated an IP address from the released subnet will be reset.

Note the following behavior for the **clear ip dhcp subnet** command:

- If you do not specify the **pool** *name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-virtual routing and forwarding (VRF) DHCP pools for the specified subnet.
- If you do not specify the **pool** *name* option and the * option is specified, it is assumed that all automatic or on-demand subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *name* option and the * option, all automatic or on-demand subnets in the specified pool only will be cleared.
- If you specify the **pool** *name* option and an IP address, the subnet containing the specified IP address will be deleted from the specified pool.

Caution Use this command with caution to prevent undesired termination of active PPP sessions.

Examples

The following example releases the subnet containing 10.0.0.2 from any non-VRF on-demand address pools:

```
Router# clear ip dhcp subnet 10.0.0.2
```

The following example clears all leased subnets from all pools:

```
Router# clear ip dhcp subnet *
```

The following example clears all leased subnets from the address pool named pool3:

```
Router# clear ip dhcp pool pool3 subnet *
```

The following example clears the address 10.0.0.2 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 subnet 10.0.0.2
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

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.

Defaults

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.

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 dotted-hexadecimal notation, for example, 01b7.0813.8811.66.

Defaults

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

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. For example, the Microsoft client identifier for Ethernet address b708.1388.f166 is 01b7.0813.88f1.66, where 01 represents the Ethernet media type. 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:

```
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.

Defaults

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

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.

Defaults

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.

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.

Defaults

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.

domain-name (DHCP)

To specify the domain name 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.

Defaults

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.

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 Table 7 for valid entries.

Defaults

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.

Table 7 lists the valid assigned hardware numbers found online at http://www.iana.org/assignments/arp-parameters.

Table 7 ARP Hardware Numbers and Types

Hardware Number	Hardware Type
1	Ethernet
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25

Table 7 ARP Hardware Numbers and Types (continued)

Hardware Number	Hardware Type
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
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 (/).

Defaults

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.

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.

Defaults

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

ip address dhcp

To acquire an IP address on an interface from the Dynamic Host Configuration Protocol (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-name*] [**hostname** *host-name*]

no ip address dhcp [**client-id** *interface-name*] [**hostname** *host-name*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-name* option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-name	(Optional) The interface name from which the MAC address is taken.
hostname	(Optional) Specifies the hostname.
host-name	(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.

Defaults

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	The **client-id** keyword and *interface-name* argument were added.
12.2(3)	The **hostname** keyword and *host-name* argument were added. The behavior of the **client-id** *interface-name* option changed. See the “Usage Guidelines” section for details.
12.2(8)T	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.

Usage Guidelines

Note Prior to 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-name* **hostname** *host-name* command is when *interface-name* is the Ethernet interface where the command is configured and *host-name* 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* 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 allowed the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forced 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 (host name option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured host name of the router. However, you can use the **ip address dhcp hostname** *host-name* 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. Table 8 shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 8 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 *host-name*	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 *host-name* 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 *host-name*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *host-name* 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 1 interface 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 1 interface 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*.

Defaults

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 dhcp aaa default username

To specify the default user name for non-virtual routing and forwarding (VRF) address pools that have been configured to obtain subnets through authentication, authorization, and accounting (AAA), use the **ip dhcp aaa default username** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp aaa default username *name*

no ip dhcp aaa default username *name*

Syntax Description

name	Name of the address pool.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The behavior when the username attribute is sent in the AAA request was changed.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Address pools that are configured with the **vrf** and **origin aaa** commands will set the username attribute in the AAA request to the specified VRF name. If the VPN ID as specified in RFC 2685 is configured for the VRF, the VPN ID will be sent instead.

Address pools that are not configured with the **vrf** command but are configured with the **origin aaa** command, will set the username attribute in the AAA request to the specified name in the **ip dhcp aaa default username** command.

Use the **debug aaa attribute** command to verify the value of the username attribute in the subnet request to the AAA server.

In Cisco IOS Release 12.2(8)T, if this command is not configured, no AAA subnet request from non-VRF ODAPs will be sent.

In Cisco IOS Release 12.2(15)T, if the DHCP pool is not configured with VRF and the **ip dhcp aaa default username** command is not configured, the AAA request will still be sent with the username attribute set to the DHCP pool name.

This command is not needed if all on-demand address pools (ODAPs) on the VHG/provider edge (PE) are VRF-associated.

Examples

The following example sets the username attribute in the AAA request to abc:

```
ip dhcp aaa default username abc
```

Related Commands

Command	Description
debug aaa attribute	Verifies the value of the AAA attributes.
origin	Configures an address pool as an on-demand address pool.
vrf	Associates the on-demand address pool with a VPN routing and forwarding instance.

ip dhcp bootp ignore

To enable a Dynamic Host Configuration Protocol (DHCP) server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, use the **ip dhcp bootp ignore** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip dhcp bootp ignore

no ip dhcp bootp ignore

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to service BOOTP requests.

Command Modes

Global configuration

Command History

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

Usage Guidelines

A DHCP server can forward ignored BOOTP request packets to another DHCP server if the **ip helper-address** command is configured on the incoming interface. If the **ip helper-address** command is not configured, the router will drop the received BOOTP request.

Examples

The following example shows that the router will ignore received BOOTP requests:

```
hostname Router
!
ip subnet-zero
!
ip dhcp bootp ignore
```

Related Commands

Command	Description
ip bootp server	Enables the BOOTP service on routing devices.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip dhcp class

To define a Dynamic Host Configuration Protocol (DHCP) class and enter DHCP class configuration mode, use the **ip dhcp class** command in global configuration mode. To remove the class, use the **no** form of this command.

ip dhcp class *class-name*

no ip dhcp class *class-name*

Syntax Description

class-name	Name of the DHCP class.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

DHCP class configuration provides a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside.

Examples

The following example defines three DHCP classes and their associated relay agent information patterns. Note that CLASS3 is considered a "match to any" class because it has no relay agent information pattern configured:

```
ip dhcp class CLASS1
 relay agent information
! Relay agent information patterns
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
 relay agent information
! Relay agent information patterns
  relay-information hex 01040102030402020102
  relay-information hex 01040101030402020102

ip dhcp class CLASS3
 relay agent information
```

Related Commands

Command	Description
relay agent information	Enters relay agent information option configuration mode.
relay-information hex	Specifies a hexadecimal string for the full relay agent information option.

ip dhcp client

To configure the Dynamic Host Configuration Protocol (DHCP) client to associate any added routes with a specified tracked object number, use the **ip dhcp client** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip dhcp client route track *number*

no ip dhcp client route track

Syntax Description

route track *number*	Associates a tracked object number with the DHCP-installed static route. Valid values for the *number* argument range from 1 to 500.

Defaults

No routes are associated with a track number.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ip dhcp client** command must be configured before the **ip address dhcp** command is configured on an interface. The **ip dhcp client** command is checked only when an IP address is acquired from DHCP. If the **ip dhcp client** command is specified after an IP address has been acquired from DHCP, the **ip dhcp client** command will not take effect until the next time the router acquires an IP address from DHCP.

Examples

The following example configures DHCP on an Ethernet interface and associates tracked object 123 with routes generated from this interface:

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.

ip dhcp client authentication key-chain

To specify the key chain to be used in authenticating a request, use the **ip dhcp client authentication key-chain** command in interface configuration mode. To disable key-chain authentication, use the **no** form of this command.

ip dhcp client authentication key-chain *name*

no ip dhcp client authentication key-chain *name*

Syntax Description

name	Name of the key chain.

Command Default

Authentication is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Configure the **ip dhcp client authentication key-chain** command to send to the server authentication messages that are encoded by the secret ID and secret value that were configured in the **key chain** command. When authentication is enabled, all client-server exchanges must be authenticated: the **ip dhcp client authentication mode** and **key chain** commands must be configured.

Examples

The following example shows how to specify a key chain named chain1 for authentication exchanges:

```
Router(config-if)# ip dhcp client authentication key-chain chain1
```

Related Commands

Command	Description
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
ip dhcp-client forcerenew	Enables forcerenew-message handling on the DHCP client when authentication is enabled.
key chain	Identifies a group of authentication keys for routing protocols.

ip dhcp client authentication mode

To specify the type of authentication to be used in DHCP messages on the interface, use the **ip dhcp client authentication mode** command in interface configuration mode. To remove the specification, use the **no** form of this command.

ip dhcp client authentication mode {**md5** | **token**}

no ip dhcp client authentication mode {md5 | token}

Syntax Description

md5	Specifies MD5-based authentication.
token	Specifies token-based authentication.

Command Default

No authentication mode is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Token-based authentication is useful only for basic protection against inadvertently instantiated DHCP servers. Tokens are transmitted in plain text; they provide weak authentication and do not provide message authentication. MD5-based authentication provides better message and entry authentication because it specifies the generation of a temporary value by the source.

Examples

The following example shows how to specify chain1 as the key chain, and MD5 as the mode, for authentication exchanges:

```
Router(config-if)# ip dhcp client authentication key-chain chain1
Router(config-if)# ip dhcp client authentication mode md5
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp-client forcerenew	Enables forcerenew-message handling on the DHCP client when authentication is enabled.
key chain	Identifies a group of authentication keys for routing protocols.

ip dhcp-client broadcast-flag

To configure the Dynamic Host Configuration (DHCP) client to set the broadcast flag, use the **ip dhcp-client broadcast-flag** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip dhcp-client broadcast-flag

no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Defaults

The broadcast flag is on.

Command Modes

Global configuration

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

Use this command to set the broadcast flag to 1 or 0 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If the **no ip dhcp-client broadcast-flag** command is entered, the broadcast flag is set to 0 and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

Examples

The following example sets the broadcast flag on:

```
ip dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface via DHCP.
service dhcp	Enables DHCP server and relay functions.

ip dhcp client class-id

To specify the class identifier, use the **ip dhcp client class-id** command in interface configuration mode. To remove the class identifier, use the **no** form of this command.

ip dhcp client class-id {*string* | **hex** *string*}

no ip dhcp client class-id {*string* | **hex** *string*}

Syntax Description

string	A unique ASCII string.
hex *string*	A unique hexadecimal value.

Defaults

No class identifier is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client class-id** command is checked only when an IP address is acquired from a Dynamic Host Configuration Protocol (DHCP) server. If the command is specified after an IP address has been acquired from the DHCP server, the command will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been specified.

The class identifier is used by vendors to specify the type of device that is requesting an IP address. For example, docsis 1.0 can be used for a cable modem and Cisco Systems, Inc. IP Phone can be used for a Cisco IP phone.

Examples

The following example configures a class identifier with a hexadecimal string of ABCDEF1235:

```
interface Ethernet 1
 ip dhcp client class-id hex ABCDEF1235
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client default-router distance

To configure the default Dynamic Host Configuration Protocol (DHCP) administrative distance, use the **ip dhcp client default-router distance** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client default-router distance *metric-value*

no ip dhcp client default-router distance

Syntax Description

metric-value	Default route metric value. Range: 1 to 255. Default: 254.

Command Default

The default administrative distance is 254.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

While you are adding the default route the administrative distance is calculated as follows:

- Interface configuration is given the highest preference if the metric value is not set to the default value.
- If a metric value is not configured on an interface, then the existing global configuration command will get preference.
- If the administrative distance is not configured in both interface configuration mode and global configuration mode, then the global configuration default distance of 254 is used.

Examples

The following example shows how to configure the DHCP default route metric to 2:

```
Router # configure terminal
Router(config)# interface FastEthernet 0/2
Router(config-if)# ip dhcp client default-router distance 2
```

Related Commands

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

Command	Description
ip dhcp-client default-router distance	Configures a default DHCP administrative distance for clients in global configuration mode.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp-client default-router distance

To configure a default Dynamic Host Configuration Protocol (DHCP) administrative distance for clients, use the **ip dhcp-client default-router distance** command in global configuration mode. To return to the default, use the **no** form of this command.

ip dhcp-client default-router distance *value*

no ip dhcp-client default-router distance *value*

Syntax Description

distance	DHCP administrative distance. The *value* argument sets the default distance. The range is from 1 to 255.

Defaults

254

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the default admininstrative distance to 25:

```
ip dhcp-client default-router distance 25
```

Related Commands

Command	Description
debug dhcp client	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp-client forcerenew

To enable forcerenew-message handling on the DHCP client when authentication is enabled, use the **ip dhcp-client forcerenew** command in global configuration mode. To disable the forced authentication, use the **no** form of this command.

ip dhcp-client forcerenew

no ip dhcp-client forcerenew

Syntax Description

This command has no arguments or keywords.

Command Default

Forcerenew messages are dropped.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

DHCP forcerenew handling is not enabled until the CLI is configured.

Examples

The following example shows how to enable DHCP forcerenew-message handling on the DHCP client:

```
Router(config)# ip dhcp-client forcerenew
```

Related Commands

Command	Description
ip dhcp client authentication key-chain	Specifies the key chain to be used in DHCP authentication requests.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
key chain	Identifies a group of authentication keys for routing protocols.

ip dhcp client hostname

To specify or modify the hostname sent in a Dynamic Host Configuration Protocol (DHCP) message, use the **ip dhcp client hostname** command in interface configuration mode. To remove the hostname, use the **no** form of this command.

ip dhcp client hostname *host-name*

no ip dhcp client hostname *host-name*

Syntax Description

host-name	Name of the host.

Command Default

The hostname is the globally configured hostname of the router.

Command Modes

Interface configuration(config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client hostname** command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been specified.

This command is applicable only for DHCP requests generated by Cisco IOS software. This command is ignored when Cisco IOS software relays requests (for example, from Distributed Route Processor PPP clients).

Examples

The following example shows how to specify the hostname of the DHCP client as hostA:

```
interface Ethernet 1
 ip dhcp client hostname hostA
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client lease

To configure the duration of the lease for an IP address that is requested from a Dynamic Host Configuration Protocol (DHCP) client to a DHCP server, use the **ip dhcp client lease** command in interface configuration mode. To restore to the default value, use the **no** form of this command.

ip dhcp client lease *days* [*hours*] [*minutes*]

no ip dhcp client lease

Syntax Description

days	Specifies the duration of the lease in days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before an *hours* value can be configured.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before a *minutes* value can be configured.

Defaults

A default lease time is not included in the DHCP DISCOVER messages sent by the client. The client accepts the lease time that the DHCP server sends.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ip dhcp client lease** command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been specified.

Examples

The following example shows a one-day lease:

```
ip dhcp client lease 1
```

The following example shows a one-hour lease:

```
ip dhcp client lease 0 1
```

The following example shows a one-minute lease:

```
ip dhcp client lease 0 0 1
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client mobile renew

To configure the number of renewal attempts and the interval between attempts for renewing an IP address acquired by a Dynamic Host Configuration Protocol (DHCP) client, use the **ip dhcp client mobile renew** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

ip dhcp client mobile renew count *number* **interval** *ms*

no ip dhcp client mobile renew count *number* **interval** *ms*

Syntax Description

count *number*	Number of attempts to renew a current IP address before starting the DHCP discovery process. The range is from 0 to 10 attempts. The default is 2 attempts.
interval *ms*	Interval to wait between renewal attempts. The range is from 1 to 1000 ms. The default is 50 ms.

Defaults

count *number*: 2
interval *ms*: 50

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Mobile DHCP clients automatically attempt to renew an existing IP address in response to certain events, such as moving between wireless access points. The number of renewal attempts, and the interval between those attempts, depending on network conditions, can be modified by using the **ip dhcp client mobile renew** command.

Examples

In the following example, the DHCP client will make four attempts to renew its current IP address with an interval of 30 milliseconds between attempts :

```
interface FastEthernet0
 ip dhcp client mobile renew count 4 interval 30
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.

ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery** command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

no ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

Syntax Description

informs *number-of-messages*	Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
discovers *number-of-messages*	Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
period *seconds*	Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

Defaults

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers** keywords are set to 0); 15-second timeout period.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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 dhcp-client network-discovery** command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform messages is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery** command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dhcp client request

To configure a Dynamic Host Configuration Protocol (DHCP) client to request an option from a DHCP server, use the **ip dhcp client request** command in interface configuration mode. To remove the request for an option, use the **no** form of this command.

ip dhcp client request *option-name*

no ip dhcp client request *option-name*

Syntax Description

option-name	The option name can be one of the following keywords: • **tftp-server-address** • **sip-server-address** • **netbios-nameserver** • **vendor-specific** • **vendor-identifying-specific** • **static-route** • **classless-static-route** • **domain-name** • **dns-nameserver** • **router** By default, all these options except **sip-server-address**, **vendor-identifying-specific**, and **classless-static-route** are requested.

Defaults

All the options are requested except **sip-server-address**, **vendor-identifying-specific**, and **classless-static-route**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(22)YB	This command was modified. The **sip-server-address**, **vendor-identifying-specific**, and **classless-static-route** keywords were added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

By default, all options except **sip-server-address**, **vendor-identifying-specific**, and **classless-static-route** are requested, so you must use the **no** form of the **ip dhcp client request** command to disable those default options, and explicitly specify any options that are not enabled by default.

Default options that are specified by the **no** form are removed from the DHCP originated address for the interface. An option can be reinserted in the list of requested options by using the same command without the **no** keyword. Multiple options can be specified on one configuration line. However, each option will appear on a separate line in the running configuration.

The **ip dhcp client request** command is checked only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from the DHCP server. This means that the new configuration will take effect only after either the **ip address dhcp** command or a DHCP lease renewal or termination that is not initiated by a **release dhcp** or a **renew dhcp** command.

Examples

The following example shows how to configure the DHCP client to remove the DNS name server from the options requested from the DHCP server:

```
no ip dhcp client request dns-nameserver
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.
ip dhcp-client forcerenew	Enables forcerenew-message handling on the DHCP client when authentication is enabled.
ip dhcp client authentication key-chain	Specifies the authentication key used for the DHCP protocol on the interface.
ip dhcp client authentication mode	Specifies the type of authentication to be used in DHCP messages on the interface.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.
Command	**Description**
ip address dhcp	Acquires an IP address on an interface from DHCP.
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp compatibility lease-query client

To configure the Dynamic Host Configuration Protocol (DHCP) client to send a lease query according to RFC 4388, use the **ip dhcp compatibility lease-query client** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip dhcp compatibility lease-query client {**cisco** | **standard**}

no ip dhcp compatibility lease-query client

Syntax Description

cisco	Configures the DHCP client to use the Cisco standard lease-query message type. This is the default value.
standard	Configures the DHCP client to use the RFC 4388 standard lease-query message type.

Command Default

The DHCP client is configured to use the Cisco standard lease-query message type.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Some DHCP servers support only the RFC 4388 standard of lease query. If the DHCP server supports only the RFC 4388 standard, then you must configure the DHCP client to send a lease query according to the RFC 4388 standard.

The Cisco IOS DHCP client sends a lease query with the message type set to 13 and receives either an ACK (acknowledge) or NAK (deny) from the DHCP server. This is the behavior of the DHCP client as per the Cisco standard.

As per the RFC 4388 standard, if a DHCP server receives a lease query with the message type set to 10, it will reply with one of the following message types:

• DHCPLEASEUNASSIGNED	11
• DHCPLEASEUNKNOWN	12
• DHCPLEASEACTIVE	13

By using the **ip dhcp compatibility lease-query client** command, you can switch between Cisco's implementation and the RFC 4388 standard implementation.

Examples

The following example shows how to configure the DHCP client to switch from Cisco's implementation to the RFC 4388 standard implementation:

```
Router(config)# ip dhcp compatibility lease-query client standard
```

Related Commands

Command	Description
ip dhcp compatibility suboption	Configures DHCP compatibility for a relay-agent suboption.

ip dhcp compatibility suboption link-selection

To configure the Dynamic Host Configuration Protocol (DHCP) client to use private as well as the Internet Assigned Numbers Authority (IANA) standard relay agent suboption numbers, use the **ip dhcp compatibility suboption link-selection** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip dhcp compatibility suboption link-selection {**cisco** | **standard**}

no ip dhcp compatibility suboption link-selection

Syntax Description

cisco	Configures the DHCP client to use the private Cisco suboption numbers.
standard	Configures the DHCP client to use the standard IANA suboption numbers.

Command Default

Disabled. (The DHCP client is configured to use the private relay agent suboption numbers.)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(100)	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Sometimes new features are implemented in advance of standardization. That is, features are developed before the IANA numbers are assigned to the relay agent suboptions. In these cases, the DHCP client uses the private Cisco relay agent suboption numbers. When the IANA numbers are assigned later, the DHCP client must be able to use both the private as well as the IANA relay suboption numbers. You can use the **ip dhcp compatibility suboption link-selection** command to configure the DHCP client to use the IANA relay agent suboption numbers.

Examples

The following example shows how to configure the DHCP client to support the relay agent with the IANA standard suboption number:

```
Router(config)# ip dhcp compatibility suboption link-selection standard
```

Related Commands

Command	Description
ip dhcp compatibility lease-query client	Configures the DHCP client to send a lease query according to the RFC 4388 standard.

ip dhcp conflict logging

To enable conflict logging on a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** command in global configuration mode. To disable conflict logging, use the **no** form of this command.

ip dhcp conflict logging

no ip dhcp conflict logging

Syntax Description

This command has no arguments or keywords.

Defaults

Conflict logging is enabled.

Command Modes

Global 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

A DHCP server database agent should be used to store automatic bindings. If a DHCP server database agent is not used, specify the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the DHCP server records DHCP address conflicts in a log file.

Examples

The following example disables the recording of DHCP address conflicts:

```
no ip dhcp conflict logging
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

ip dhcp conflict resolution

To configure Dynamic Host Configuration Protocol (DHCP) address conflict resolution, use the **ip dhcp conflict resolution** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp conflict resolution [**interval** *minutes*]

no ip dhcp conflict resolution

Syntax Description

interval *minutes*	(Optional) Specifies the time interval, in minutes. Range: 5 to 1440. Default: 60.

Command Default

DHCP address conflict resolution is disabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

DHCP addresses added to the conflicted address list may become available after some time. This behavior will eventually cause a major chunk of the IP addresses that are actually available to be blocked.

You can use the **ip dhcp conflict resolution** command to configure the DHCP server to periodically audit the conflicted address list and clear the inactive IP addresses.

Examples

The following example shows how to configure address conflict resolution on a DHCP server to take place after 65 minutes:

```
Router # configure terminal
Router(config)# ip dhcp conflict resolution interval 65
```

Related Commands

Command	Description
ip dhcp conflict logging	Enables conflict logging on a DHCP server.

ip dhcp database

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent to save automatic bindings on a remote host called a database agent, use the **ip dhcp database** command in global configuration mode. To remove the database agent, use the **no** form of this command.

ip dhcp database *url* [**timeout** *seconds* | **write-delay** *seconds* | **write-delay** *seconds* **timeout** *seconds*]

no ip dhcp database *url*

Syntax Description

url	Specifies the remote file used to store the automatic bindings. The following are acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
timeout *seconds*	(Optional) Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. By default, DHCP waits 300 seconds (5 minutes) before aborting a database transfer. Infinity is defined as 0 seconds.
write-delay *seconds*	(Optional) Specifies how soon the DHCP server should send database updates. By default, DHCP waits 300 seconds (5 minutes) before sending database changes. The minimum delay is 60 seconds.

Defaults

DHCP waits 300 seconds for both a write delay and a timeout.

Command Modes

Global 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

A DHCP database agent is any host (for example, an FTP, TFTP, or rcp server) or storage media on the DHCP server (for example, disk0) that stores the DHCP bindings database. You can configure multiple DHCP database agents, and you can configure the interval between database updates and transfers for each agent.

The DHCP relay agent can save route information to the same database agents to ensure recovery after reloads.

In the following example, the timeout value and write-delay are specified in two separate command lines:

```
ip dhcp database disk0:router-dhcp timeout 60
ip dhcp database disk0:router-dhcp write-delay 60
```

However, the second configuration overrides the first command line and causes the timeout value to revert to the default value of 300 seconds. To prevent the timeout value from reverting to the default value, configure the following on one command line:

```
ip dhcp database disk0:router-dhcp write-delay 60 timeout 60
```

Examples

The following example specifies the DHCP database transfer timeout value as 80 seconds:

```
ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80
```

The following example specifies the DHCP database update delay value as 100 seconds:

```
ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100
```

Related Commands

Command	Description
show ip dhcp database	Displays Cisco IOS DHCP server database agent information.

ip dhcp excluded-address

To specify IP addresses that a Dynamic Host Configuration Protocol (DHCP) server should not assign to DHCP clients, use the **ip dhcp excluded-address** command in global configuration mode. To remove the excluded IP addresses, use the **no** form of this command.

ip dhcp excluded-address [**vrf** *vrf-name*] *ip-address* [*last-ip-address*]

no ip dhcp excluded-address [**vrf** *vrf-name*] *ip-address* [*last-ip-address*]

Syntax Description

vrf	(Optional) Excludes IP addresses from a virtual routing and forwarding (VRF) space.
vrf-name	(Optional) The VRF name.
ip-address	The excluded IP address, or first IP address in an excluded address range.
last-ip-address	(Optional) The last IP address in the excluded address range.

Command Default

The DHCP server can assign any IP address to the DHCP clients.

Command Modes

Global configuration (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.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Use the **ip dhcp excluded-address** command to exclude a single IP address or a range of IP addresses.

The DHCP server assumes that all pool addresses can be assigned to the clients. You cannot use the **ip dhcp excluded-address** command to stop the DHCP server from assigning the pool addresses (assigned to an interface using the **ip address pool** command) to the clients. That is, the **ip dhcp excluded-address** command is not supported for the addresses assigned using the **ip address pool** command.

Examples

The following example shows how to configure an excluded IP address range from 172.16.1.100 through 172.16.1.199:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp excluded-address vrf vrf1 172.16.1.100 172.16.1.199
```

Related Commands

Command	Description
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.
ip address pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.

ip dhcp limit lease

To limit the number of leases offered to DHCP clients per interface, use the **ip dhcp limit lease** command in interface configuration mode. To remove the restriction on the number of leases, use the **no** form of this command.

ip dhcp limit lease *lease-limit*

no ip dhcp limit lease *lease-limit*

Syntax Description

lease-limit	Number of leases allowed on the interface. The range is from 1 to 65535.

Command Default

There is no lease limit on an interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The lease limit allows you to control the number of subscribers per interface. The interface configuration will override any global setting specified by the **ip dhcp limit lease per interface** command. You can display the number of lease violations by using the **show ip dhcp limit lease** command.

This command is not supported on numbered interfaces. The lease limit can be applied only to an ATM with Routed Bridge Encapsulation (RBE) unnumbered interfaces or serial unnumbered interfaces.

Examples

The following example allows 30 DHCP clients to receive IP addresses. If a 31st DHCP client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server.

```
!
Router(config)# ip dhcp limit lease log
Router(config)# interface Serial0/0
Router(config-if)# ip dhcp limit lease 30
```

Related Commands

Command	Description
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip dhcp limit lease log

To enable DHCP lease violation logging when a DHCP lease limit threshold is exceeded, use the **ip dhcp limit lease log** command in global configuration mode. To disable the lease violation logging of DHCP lease violations, use the **no** form of this command.

ip dhcp limit lease log

no ip dhcp limit lease log

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP lease violation logging is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ip dhcp limit lease log** command logs violations for global- and interface-level lease violations. If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.

Examples

The following example shows how to enable logging of lease violations:

```
Router(config)# ip dhcp limit lease log
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip dhcp limit lease per interface

To limit the number of leases offered to DHCP clients behind an ATM routed bridge encapsulation (RBE) unnumbered or serial unnumbered interface, use the **ip dhcp limit lease per interface** command in global configuration mode. To remove the restriction on the number of leases, use the **no** form of the command.

ip dhcp limit lease per interface *lease-limit*

no ip dhcp limit lease per interface *lease-limit*

Syntax Description

lease-limit	Number of leases allowed. The range is from 1 to 65535.

Command Default

The number of leases offered is not limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

This command is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.

Examples

The following example shows how to allow three DHCP clients to receive IP addresses. If a fourth DHCP client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server.

```
Router(config)# ip dhcp limit lease per interface 3
```

Related Commands

Command	Description
clear ip dhcp limit lease	Clears the stored lease violation entries.
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated.

ip dhcp limited-broadcast-address

To override a configured network broadcast and have the Dynamic Host Configuration Protocol (DHCP) server and relay agent send an all networks, all nodes broadcast to a DHCP client, use the **ip dhcp limited-broadcast-address** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp limited-broadcast-address

no ip dhcp limited-broadcast-address

Syntax Description

This command has no arguments or keywords.

Defaults

Default broadcast address: 255.255.255.255 (all ones)

Command Modes

Global configuration

Command History

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

Usage Guidelines

When a DHCP client sets the broadcast bit in a DHCP packet, the DHCP server and relay agent send DHCP messages to clients using the all ones broadcast address (255.255.255.255). If the **ip broadcast-address** command has been configured to send a network broadcast, the all ones broadcast set by DHCP is overridden. To remedy this situation, use the **ip dhcp limited-broadcast-address** command to ensure that a configured network broadcast does not override the default DHCP behavior.

Some DHCP clients can only accept an all ones broadcast and may not be able to acquire a DHCP address unless this command is configured on the router interface connected to the client.

Examples

The following example configures DHCP to override any network broadcast:

```
ip dhcp limited-broadcast-address
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.

ip dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol (DHCP) server sends to a pool address as part of a ping operation, use the **ip dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command. To return the number of ping packets sent to the default value, use the **default** form of this command.

ip dhcp ping packets *number*

no ip dhcp ping packets

default ip dhcp ping packets

Syntax Description

number	The number of ping packets that are sent before the address is assigned to a requesting client. The default value is two packets.

Defaults

Two packets

Command Modes

Global 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 DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to a value of 0 completely turns off DHCP server ping operation .

Examples

The following example specifies five ping attempts by the DHCP server before ceasing any further ping attempts:

```
ip dhcp ping packets 5
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP Server waits for a ping reply from an address pool.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

ip dhcp ping timeout

To specify how long a Dynamic Host Configuration Protocol (DHCP) server waits for a ping reply from an address pool, use the **ip dhcp ping timeout** command in global configuration mode. To restore the default number of milliseconds (500) of the timeout, use the **no** form of this command.

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Syntax Description

milliseconds	The amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The maximum timeout is 10000 milliseconds (10 seconds). The default timeout is 500 milliseconds.

Defaults

500 milliseconds

Command Modes

Global 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 specifies how long to wait for a ping reply (in milliseconds).

Examples

The following example specifies that a DHCP server will wait 800 milliseconds for a ping reply before considering the ping a failure:

```
ip dhcp ping timeout 800
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp ping timeout	Specifies the number of packets a Cisco IOS DHCP Server sends to a pool address as part of a ping operation.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the **no** form of this command.

ip dhcp pool *name*

no ip dhcp pool *name*

Syntax Description

name	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).

Defaults

DHCP address pools are not configured.

Command Modes

Global 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

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ip dhcp relay bootp ignore

To configure the Dynamic Host Configuration Protocol (DHCP) relay agent stop forwarding Bootstrap Protocol (BOOTP) packets between the clients and servers, use the **ip dhcp relay bootp ignore** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp relay bootp ignore

no ip dhcp relay bootp ignore

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (Relay agent forwards BOOTP packets from clients and servers).

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

You can use the **ip dhcp relay agent bootp ignore** command in network deployments, where clients send both BOOTP and DHCP packets. When the client sends both type of packets, sometimes the DHCP server or the relay agent will not be able to differentiate between the two types of packets. You can use this command to configure the relay agent stop forwarding the BOOTP packets.

Examples

The following example shows how to configure the relay agent to stop forwarding BOOTP packets:

```
Router# configure terminal
Router(config)# ip dhcp relay bootp ignore
```

Related Commands

Command	Description
ip dhcp relay information	Configures a DHCP server to validate the relay agent information option.
ip dhcp bootp ignore	Configures the DHCP server to stop processing BOOTP packets from clients.

ip dhcp relay information check

To configure a Dynamic Host Configuration Protocol (DHCP) server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check** command in global configuration mode. To disable an information check, use the **no** form of this command.

ip dhcp relay information check

no ip dhcp relay information check

Syntax Description

This command has no arguments or keywords.

Defaults

A DHCP server checks relay information. Invalid messages are dropped.

Command Modes

Global 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 used by cable access router termination systems. By default, DHCP checks relay information. Invalid messages are dropped.

Examples

The following example configures the DHCP Server to check that the relay agent information option in forwarded BOOTREPLY messages is valid:

```
ip dhcp relay information check
```

Related Commands

Command	Description
ip dhcp relay information option	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

ip dhcp relay information check-reply

To configure a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check-reply** command in interface or subinterface configuration mode. To disable an information check, use the **no** form of this command.

ip dhcp relay information check-reply [**none**]

no ip dhcp relay information check-reply [**none**]

Syntax Description

none	(Optional) Disables the command function.

Command Default

A DHCP server checks relay information. Invalid messages are dropped.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information check-reply none** command option is saved in the running configuration. This command takes precedence over any relay agent information global configuration.

Examples

The following example shows how to configure the DHCP server to check that the relay agent information option in forwarded BOOTREPLY messages received from FastEthernet interface 0 is valid:

```
!
interface FastEthernet 0
 ip dhcp relay information check-reply
```

Related Commands

Command	Description
ip dhcp relay information option-insert	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information check	Configures a DHCP server to validate the relay information option in forwarded BOOTREPLY messages in global configuration mode.
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent.

ip dhcp relay information option

To enable the system to insert a Dynamic Host Configuration Protocol (DHCP) relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option** command in global configuration mode. To disable inserting relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

ip dhcp relay information option [**vpn**]

no ip dhcp relay information option [**vpn**]

Syntax Description

vpn	(Optional) Virtual private network.

Command Default

The DHCP server does not insert relay information.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(4)B	The **vpn** keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 functionality enables a DHCP server to identify the user (for example, cable access router) sending a request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.

The **ip dhcp relay information option** command automatically adds the circuit identifier suboption and the remote ID suboption to the DHCP relay agent information option (also called option 82).

The **vpn** optional keyword should be used only when the DHCP server allocates addresses based on VPN identification suboptions.

The **ip dhcp relay information option vpn** command adds the following VPN-related suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- VPN identifier—Contains the VPN ID if configured or the virtual routing and forwarding (VRF) name if configured on the interface (VPN ID takes precedence over VRF name).
- Subnet selection—Contains the incoming interface subnet address.
- Server identifier override—Contains the incoming interface IP address.

After these suboptions are successfully added, the gateway address is set to the outgoing interface of the router toward the DHCP server IP address that was configured using the **ip helper-address** command.

If only the **ip dhcp relay information option vpn** command is configured, the VPN identifier, subnet selection, and server identifier override suboptions are added to the relay information option. Note that the circuit identifier suboption and the remote ID suboption are not added to the relay information option. However, if both the **ip dhcp relay information option** command and the **ip dhcp relay information option vpn** command are configured, all five suboptions are added to the relay agent information option.

When the packets are returned from the DHCP server, option 82 is removed before the reply is forwarded to the client.

Even if the **vpn** option is specified, the VPN suboptions are added only to those DHCP or BOOTP broadcasts picked up by the interface that was configured with a VRF name or VPN ID.

For clients from unnumbered ATM or serial interfaces, when this command is enabled, the VPN identifier suboption will contain the VRF name of the unnumbered interface.

Subnet selection and server identifier override suboptions are added from the IP address of the interface from which the unnumbered interface is configured to borrow its IP address. The client host route will be added on the applicable VRF routing tables.

If the **ip dhcp smart-relay** global configuration command is enabled, then the server identifier override and subnet selection suboptions will use the secondary IP address of the incoming interface when the same client retransmits more than three DHCP DISCOVER packets (for both numbered and unnumbered interfaces).

Examples

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, in forwarded BOOTREQUEST messages. In this example, the circuit identifier suboption and the remote ID suboption are not included in the relay information option:

```
ip dhcp relay information option vpn
```

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, the circuit identifier suboption, and the remote ID suboption, in forwarded BOOTREQUEST messages:

```
ip dhcp relay information option vpn
ip dhcp relay information option
```

Cisco 10000 Series Router

The following example enables DHCP option 82 support on the DHCP relay agent by using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. The value (in hexadecimal) of the agent remote ID suboption is 010100000B0101814058320, and the value of each field is the following:

- Port Type: 0x01
- Version: 0x01
- Reserved: undefined
- NAS IP address: 0x0B010181 (hexadecimal value of 11.1.1.129)

- NAS Port
  - Interface (slot/module/port): 0x40 (The slot/module/port values are 01 00/0/000.)
  - VPI: 0x58 (hexadecimal value of 88)
  - VCI: 0x320 (hexadecimal value of 800)

```
ip dhcp-server 172.16.1.2
!
ip dhcp relay information option
!
interface Loopback0
    ip address 10.1.1.129 255.255.255.192
!
interface ATM4/0
    no ip address
!
interface ATM4/0.1 point-to-point
    ip unnumbered Loopback0
    ip helper-address 172.16.1.2
    atm route-bridged ip
    pvc 88/800
        encapsulation aal5snap
!
interface Ethernet 5/1
    ip address 172.16.1.1 255.255.0.0
!
router eigrp 100
    network 10.0.0.0
    network 172.16.0.0
!
rbe nasip Loopback0
```

In the following example, the DHCP relay receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named *red*.

```
ip dhcp relay information option vpn
!
interface ethernet 0/1
    ip helper-address vrf red 10.44.23.7
```

Related Commands

Command	Description
Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent.
ip dhcp smart-relay	Allows the Cisco IOS DHCP relay agent to switch the gateway address.

ip dhcp relay information option-insert

To enable the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option-insert** command in interface configuration mode or subinterface configuration mode. To disable inserting relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

ip dhcp relay information option-insert [**none**]

no ip dhcp relay information option-insert [**none**]

Syntax Description

none	(Optional) Disables the command function.

Command Default

The DHCP server does not insert relay information.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information option-insert none** command option is saved in the running configuration. This command takes precedence over any relay agent information global configuration.

Examples

The following example shows how to configure the DHCP server to insert the relay agent information option in forwarded BOOTREQUEST messages:

```
!
interface FastEthernet 0
 ip dhcp relay information option-insert
```

Related Commands

Command	Description
ip dhcp relay information check-reply	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server in global configuration mode.
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent.

ip dhcp relay information option server-id-override

To enable the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp relay information option server-id-override** command in interface configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the no form of this command.

ip dhcp relay information option server-id-override

no ip dhcp relay information option server-id-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ip dhcp relay information option server-id-override** interface configuration command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** interface configuration command is configured on an interface, it overrides the **ip dhcp-relay information option server-override** global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option on interface Ethernet interface 0/0.

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip dhcp relay information option server-id-override
```

Related Commands

Command	Description
ip dhcp-relay information option server-override	Enables the system to globally insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the no form of this command.

ip dhcp-relay information option server-override

no ip dhcp-relay information option server-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** interface configuration command is configured on an interface, it overrides the global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
!
Router(config)# ip dhcp-relay information option server-override
Router(config)# ip dhcp-relay source-interface loopback0
!
Router(config)# interface Loopback0
Router(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay information option server-id-override	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp relay information option subscriber-id

To specify that a Dynamic Host Configuration Protocol (DHCP) relay agent add a subscriber identifier suboption to option82, use the **ip dhcp relay information option subscriber-id** command in interface configuration mode. To disable the subscriber identifier, use the **no** form of this command.

ip dhcp relay information option subscriber-id *string*

no ip dhcp relay information option subscriber-id *string*

Syntax Description

string	Up to a maximum of 50 characters that can be alphanumeric. The string can be ASCII text only. **Note** If more than 50 characters are configured, the string is truncated.

Defaults

Disabled to allow backward capability.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When the unique subscriber identifier is configured on the relay agent and the interface, the identifier is added to option82 in all of the client DHCP packets to the DHCP server. When the server echoes option82 in the reply packets, the relay agent removes option82 before forwarding the reply packet to the client. When an interface is numbered, all renew packets and release packets are unicast to the server, so option82 is not added.

The unique identifier should be configured for each subscriber and when a subscriber moves from one interface to the other, the configuration of the interface should be changed also.

In case of unnumbered interfaces, all the client packets are sent to the relay. Option82 is added in all the client packets before forwarding the packets to the server. If the server does not echo option82 in the packet, the relay agent tries to validate option82 in the reply packet. If the reply packet does not contain option82, then the validation fails and the packet is dropped by the relay agent. The client cannot get any IP address because of the validation failure. In this case, the existing **no ip dhcp relay information check** command can be used to avoid the option82 invalidation.

Note The configurable string is not an option for network access server (NAS)-IP, because users can move between NAS termination points. When a subscriber moves from one NAS to another, this option does not result in a configuration change on the side of the DHCP server of the ISP.

Examples

The following example shows how to configure an ATM interface for the subscriber identifier suboption.

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM4/0
 no ip address
!
interface ATM4/0.1 point-to-point
 ip helper-address 10.16.1.2
 ip unnumbered Loopback0
 ip dhcp relay information option subscriber-id newperson123
 atm route-bridged ip
 pvc 88/800
 encapsulation aal5snap
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).
ip dhcp smart-relay	Enables the Cisco IOS DHCP relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip dhcp relay information option vpn-id

To enable the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and set the gateway address to the outgoing interface toward the DHCP server, use the **ip dhcp relay information option vpn-id** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip dhcp relay information option vpn-id [**none**]

no ip dhcp relay information option vpn-id

Syntax Description

none	(Optional) Disables the VPN functionality on the interface.

Command Default

The DHCP server does not insert relay information.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id** interface configuration command is not configured, the global configuration is applied to all interfaces.

If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id** interface configuration command is also configured, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If the **ip dhcp relay information option vpn** global configuration command is not configured and the **ip dhcp relay information option vpn-id** interface configuration command is configured, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information option vpn-id none** option allows you to disable the VPN functionality on the interface. The only time you need to use this option is when the **ip dhcp relay information option vpn** global configuration command is configured and you want to override the global configuration.

The **no ip dhcp relay information option vpn-id** command removes the configuration from the running configuration. In this case, the interface inherits the global configuration, which may or may not be configured to insert VPN suboptions.

Examples

In the following example, the DHCP relay agent receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named red. The **ip dhcp relay information option vpn-id** interface configuration command only applies to Ethernet interface 0/1. All other interfaces are not impacted by the configuration:

```
!
interface ethernet 0/1
 ip helper-address vrf red 10.44.23.7
 ip dhcp relay information option vpn-id
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp relay information policy

To configure the information reforwarding policy for a Dynamic Host Configuration Protocol (DHCP) relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy** command in global configuration mode. To restore the default relay information policy, use the **no** form of this command.

ip dhcp relay information policy {**drop** | **encapsulate** | **keep** | **replace**}

no ip dhcp relay information policy

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
encapsulate	Encapsulates prior relay agent information.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Command Default

The DHCP server replaces existing relay information.

Command Modes

Global configuration (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.
12.2(33)SRD	This command was modified. The **encapsulate** keyword was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced.

The **ip dhcp relay information policy encapsulate** command option is only needed when the relay agent needs to encapsulate the relay agent information option from a prior relay agent. If this command option is used, the prior option 82 is encapsulated inside the current option 82 and both are forwarded to the DHCP server.

Examples

The following examples show how to configure a DHCP relay agent to drop messages with existing relay information, keep existing information, replace existing information, and encapsulate existing information, respectively:

```
ip dhcp relay information policy drop

ip dhcp relay information policy keep

ip dhcp relay information policy replace

ip dhcp relay information policy encapsulate
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Configures a Cisco IOS DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent in interface configuration mode.

ip dhcp relay information policy-action

To configure the information reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy-action** command in interface configuration mode or subinterface configuration mode. To restore the default relay information policy, use the **no** form of this command.

ip dhcp relay information policy-action {**drop** | **encapsulate** | **keep** | **replace**}

no ip dhcp relay information policy-action

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
encapsulate	Encapsulates prior information.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Command Default

The DHCP server replaces existing relay information.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was modified. The **encapsulation** keyword was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.

If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

The **ip dhcp relay information policy-action encapsulate** command is only needed when the relay agent needs to encapsulate the relay agent information option from a prior relay agent. If this command option is used, the prior option 82 is encapsulated inside the current option 82 and both are forwarded to the DHCP server.

Examples

The following example shows how to configure a DHCP relay agent to drop messages with existing relay information:

```
Router# configure terminal
Router(config)# interface FastEthernet 0
Router(config-if)# ip dhcp relay information policy-action drop
```

The following example shows how to configure a DHCP relay agent to encapsulate existing relay information:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip dhcp relay information policy-action encapsulate
```

Related Commands

Command	Description
ip dhcp relay information check-reply	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option-insert	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
ip dhcp relay information policy	Configures the information reforwarding policy for a DHCP relay agent in global configuration mode.

ip dhcp relay information trust-all

To configure all interfaces on a router as trusted sources of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trust-all** command in global configuration mode. To restore the interfaces to their default behavior, use the **no** form of the command.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Syntax Description

This command has no arguments or keywords.

Defaults

All interfaces on the router are considered untrusted.

Command Modes

Global configuration

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

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trust-all** command is configured globally, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, all interfaces on the router are configured as a trusted source for relay agent information:

```
ip dhcp relay information trust-all
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp relay information trusted

To configure an interface as a trusted source of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trusted** command in interface configuration mode. To restore the interface to the default behavior, use the **no** form of the command.

ip dhcp relay information trusted

no ip dhcp relay information trusted

Syntax Description

This command has no arguments or keywords.

Defaults

All interfaces on the router are considered untrusted.

Command Modes

Interface configuration

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

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trusted** command is configured on an interface, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, interface Ethernet 1 is configured as a trusted source for the relay agent information:

```
interface ethernet 1
 ip dhcp relay information trusted
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp relay prefer known-good-server

To configure the Dynamic Host Configuration Protocol (DHCP) relay agent to forward the client requests to the server that handled the previous request, use the **ip dhcp relay prefer known-good-server** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp relay prefer known-good-server

no ip dhcp relay prefer known-good-server

Syntax Description

This command has no arguments or keywords.

Command Default

The relay agent does not forward the requests based on the preference.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The DHCP servers send addresses to the DHCP clients. Because the DHCP server that responds first cannot be predicted, the client receives different addressees from the servers. This results in unpredictable changes in the address used by the client. Such address changes result in TCP service interruptions. You can configure the **ip dhcp relay prefer known-good-server** command to reduce the frequency with which the DHCP clients change their address and to forward the client requests to the server that handled the previous request.

If the **ip dhcp relay prefer known-good-server** command is configured, and the DHCP client is attached to an unnumbered interface, then the DHCP relay checks if the DHCP client broadcasts the DHCP packets. If the packets are broadcast, the server unicasts the requests to all configured helper addresses, and not just to the server that handled the previous request. If the packets are unicast, the DHCP relay forwards the unicast packets from the client to the DHCP server that had assigned the IP address to the client.

This functionality impacts the DHCPv4 relay, and not the DHCPv6 relay.

Examples

The following example shows how to configure the DHCP relay agent to forward the client requests to the server that handled the previous request:

```
Router# configure terminal
Router(config)# ip dhcp relay prefer known-good-server
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.

ip dhcp relay source-interface

To configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp relay source-interface** command in interface configuration mode. To remove the source interface configuration, use the **no** form of the command.

ip dhcp relay source-interface *type number*

no ip dhcp relay source-interface *type number*

Syntax Description

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

Command Default

The source interface is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ip dhcp relay source-interface** interface configuration command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** interface configuration command is also configured, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages on interface GigabitEthernet interface 0:

```
!
Router(config)# interface loopback0
Router(config-if)# ip address 10.2.2.1 255.255.255.0
!
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip dhcp relay source-interface loopback0
```

Related Commands

Command	Description
ip dhcp-relay source-interface	Globally configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of the command.

ip dhcp-relay source-interface *type number*

no ip dhcp-relay source-interface *type number*

Syntax Description

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

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ip dhcp-relay source-interface** global configuration command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** interface configuration command is also configured, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages.

```
!
Router(config)# ip dhcp-relay source-interface loopback0
!
Router(config)# interface loopback0
Router(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip dhcp route connected

To specify routes as connected routes, use the **ip dhcp route connected** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip dhcp route connected

no ip dhcp route connected

Syntax Description

This command has no arguments or keywords.

Defaults

All interfaces on the router are untrusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF	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

If you enable the **ip dhcp route connected** command, DHCP downloads the route database from a database agent and adds the routes as connected routes, even though they may have been added as static routes previously.

Examples

This example shows how to specify routes as connected routes:

```
Router(config)# ip dhcp route connected
```

ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, or to specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** command in global configuration mode. To remove a DHCP server IP address, use the **no** form of this command.

ip dhcp-server [*ip-address* | *name*]

no ip dhcp-server [*ip-address* | *name*]

Syntax Description

ip-address	(Optional) IP address of a DHCP server.
name	(Optional) Name of a DHCP server.

Defaults

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default allows automatic detection of DHCP servers.

Command Modes

Global configuration

Command History

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

Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to specify which DHCP servers are used on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.

Note To facilitate transmission, configure intermediary routers (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server. Refer to the chapters about configuring IP addressing in the *Cisco IOS IP Addressing Services Configuration Guide*.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Examples

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show cot dsp	Displays information about the COT DSP configuration or current status.

ip dhcp-server query lease

To change the default global retransmission scheme for Dynamic Host Configuration Protocol (DHCP) lease query packets, use the **ip dhcp-server query lease** command in global configuration mode. To remove this retransmission scheme and return to the default behavior, use the **no** form of this command.

ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}

no ip dhcp-server query lease {**retries** *number* | **timeout** *seconds*}

Syntax Description

retries *number*	The number of times the DHCP lease is transmitted following a timeout for an authoritative reply. The range is from 0 to 5. The default is 2 retries. A value of 0 means no retransmission (a single failure).
timeout *seconds*	The number of seconds to wait for a reply to a query. The range is from 1 to 60 seconds. The default is 5 seconds

Defaults

retries *number* : 2
timeout *seconds* : 5

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The DHCP Lease Query protocol is a lightweight mechanism to query a DHCP server for certain information related to IP addresses leased from the DHCP server.

You can specify which DHCP servers to query by using the **ip dhcp-server** global configuration command. You can specify up to 10 servers on the network. Use the **ip dhcp-server query lease** global configuration command to change the default global retransmission scheme for lease query packets.

Examples

In the following example, the time to wait for a reply to a lease query is set to 15 seconds:

```
ip dhcp-server query lease timeout 15
```

In the following example, the retry number is set to 0, which means that only a single DHCP lease query will be transmitted for each DHCP server; no retries will be attempted.

```
ip dhcp-server query lease retries 0
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP server to use on your network.

ip dhcp use

To control what information the Dynamic Host Configuration Protocol (DHCP) server accepts or rejects during address allocation, use the **ip dhcp use** command in global configuration mode. To disable the use of these parameters during address allocation, use the **no** form of this command.

ip dhcp use {**class** [**aaa**] | **vrf** {**connected** | **remote**}}

no ip dhcp use {**class** [**aaa**] | **vrf** {**connected** | **remote**}}

Syntax Description

class	Specifies that the DHCP server use DHCP classes during address allocation.
aaa	(Optional) Specifies to use the authentication, authorization, and accounting (AAA) server to get class name.
vrf	Specifies whether the DHCP server ignores or uses the receiving VPN routing and forwarding (VRF) interface during address allocation.
connected	Specifies that the server should use the VRF information from the receiving interface when servicing a directly connected client.
remote	Specifies that the server should use the VRF information from the receiving interface when servicing a request forwarded by a relay agent.

Command Default

The DHCP server allocates addresses by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When the Cisco IOS DHCP server code is allocating addresses, you can use the **ip dhcp use** command to either enable or disable the use of VRF configured on the interface, or to configure DHCP classes. If you use the **no ip dhcp use class** command, the DHCP class configuration is not deleted.

Examples

The following example shows how to configure the DHCP server to use the relay agent information option during address allocation:

```
Router(config)# ip dhcp use class
```

The following example shows how to configure the DHCP server to disable the use of the VRF information option during address allocation:

```
Router(config)# no ip dhcp use vrf connected
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

ip dhcp use subscriber-id client-id

To configure the Dynamic Host Configuration Protocol (DHCP) server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages, use the **ip dhcp use subscriber-id client-id** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp use subscriber-id client-id

no ip dhcp use subscriber-id client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP uses the client identifier option in the DHCP packet to identify clients.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A subscriber ID value configured on a specific interface using the **ip dhcp server use subscriber-id client-id** command takes precedence over this command.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
ip dhcp server use subscriber-id client id	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface.

ip dhcp smart-relay

To allow the Cisco IOS Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** command in global configuration mode. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

ip dhcp smart-relay

no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The DHCP relay agent attempts to forward the primary address as the gateway address three times. After three attempts and no response, the relay agent automatically switches to secondary addresses.

Examples

The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
ip dhcp smart-relay
```

ip dhcp snooping

To globally enable DHCP snooping, use the **ip dhcp snooping** command in global configuration mode. To disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping

no ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

```
Router(config) # ip dhcp snooping
```

This example shows how to disable DHCP snooping:

```
Router(config) # no ip dhcp snooping
```

Related Commands

Command	Description
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping binding

To set up and generate a DHCP binding configuration to restore bindings across reboots, use the **ip dhcp snooping binding** command in privileged EXEC mode. To disable the binding configuration, use the **no** form of this command.

ip dhcp snooping binding *mac-address* **vlan** *vlan ip-address* **interface** *type number* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan ip-address* **interface** *type number*

Syntax Description

mac-address	MAC address.
vlan *vlan*	Specifies a valid VLAN number; valid values are from 1 to 4094.
ip-address	IP address.
interface *type*	Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**.
number	Module and port number.
expiry *seconds*	Specifies the interval after which binding is no longer valid; valid values are from 1 to 4294967295 seconds.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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

When you add or remove a binding using this command, the binding database is marked as changed and a write is initiated.

Examples

This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Router# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 
1000
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

ip dhcp snooping database {**bootflash:***url* | **ftp:***url* | **rcp:***url* | **scp:***url* | **sup-bootflash:** | **tftp:***url* | **timeout** *seconds* | **write-delay** *seconds*}

no ip dhcp snooping database {**timeout** *seconds* | **write-delay** *seconds*}

Syntax Description

bootflash:*url*	Specifies the database URL for storing entries using the bootflash.
ftp:*url*	Specifies the database URL for storing entries using FTP.
rcp:*url*	Specifies the database URL for storing entries using remote copy (rcp).
scp:*url*	Specifies the database URL for storing entries using Secure Copy (SCP).
sup-bootflash:	Specifies the database URL for storing entries using the supervisor bootflash.
tftp:*url*	Specifies the database URL for storing entries using TFTP.
timeout *seconds*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Defaults

The DHCP-snooping database is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF5	The **sup-bootflash:** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

Examples

This example shows how to specify the database URL using TFTP:

```
Router(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Router(config)# ip dhcp snooping database write-delay 15
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping information option

To enable Dynamic Host Configuration Protocol (DHCP) option 82 data insertion, use the **ip dhcp snooping information option** command in global configuration mode. To disable DHCP option 82 data insertion, use the **no** form of this command.

ip dhcp snooping information option [**allow-untrusted**]

no ip dhcp snooping information option

Syntax Description

allow-untrusted	(Optional) Enables the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch.

Defaults

DHCP option 82 data insertion is enabled by default. Accepting incoming DHCP snooping packets with option 82 information from the edge switch is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF2	The **allow-untrusted** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

DHCP option 82 is part of RFC 3046. DHCP is an application-layer protocol that is used for the dynamic configuration of TCP/IP networks. The protocol allows for a relay agent to pass DHCP messages between the DHCP clients and DHCP servers. By using a relay agent, servers need not be on the same network as the clients. Option 82 (82 is the option’s code) addresses the security and scalability issues. Option 82 resides in the relay agent when DHCP packets that originate from the forwarding client are sent to the server. Servers that recognize Option 82 may use the information to implement the IP address or other parameter assignment policies. The DHCP server echoes the option back to the relay agent in its replies. The relay agent strips out the option from the relay agent before forwarding the reply to the client.

When you enter the **ip dhcp snooping information option allow-untrusted** on an aggregation switch that is connected to an edge switch through an untrusted interface, the aggregation switch accepts packets with option 82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. You can enable the DHCP security features, such as dynamic Address Resolution Protocol (ARP) inspection or IP source guard, on the aggregation switch while the switch receives packets with option 82 information on untrusted input interfaces to which hosts are connected. You must configure the port on the edge switch that connects to the aggregation switch as a trusted interface.

Caution Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch that is connected to an untrusted device. If you enter this command, an untrusted device might spoof the option 82 information.

Examples

This example shows how to enable DHCP option 82 data insertion:

```
ip dhcp snooping information option
```

This example shows how to disable DHCP option 82 data insertion:

```
no ip dhcp snooping information option
```

This example shows how to enable the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch:

```
ip dhcp snooping information option allow-trusted
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping limit rate

To configure the number of the DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** command in interface configuration mode. To disable the DHCP message rate limiting, use the **no** form of this command.

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

Syntax Description

rate	Number of DHCP messages that a switch can receive per second; valid values are from 1 to 4294967294 seconds.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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 Layer 2 switch-port and port-channel interfaces only.

Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interfaces, note that the trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.

Examples

This example shows how to specify the number of DHCP messages that a switch can receive per second:

```
Router(config-if)# ip dhcp snooping limit rate 150
```

This example shows how to disable the DHCP message rate limiting:

```
Router(config-if)# no ip dhcp snooping limit rate
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping packets

To enable DHCP snooping on the tunnel interface, use the **ip dhcp snooping packets** command in interface configuration mode. To disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping packets

no ip dhcp snooping packets

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	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 Layer 2 switch-port and port-channel interfaces only.

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

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

```
Router(config-if)# ip dhcp snooping packets
```

This example shows how to disable DHCP snooping:

```
Router(config-if)# no ip dhcp snooping packets
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping.
show ip dhcp snooping	Displays the DHCP snooping configuration.

Command	Description
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping verify mac-address

To verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify mac-address** command in global configuration mode. To disable verification, use the **no** form of this command.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

For untrusted DHCP snooping ports, DHCP snooping verifies the MAC address on the client hardware address field to ensure that a client is requesting multiple addresses from a single MAC address. You can use the **ip dhcp snooping verify mac-address** command to trust the ports or you can use the **no ip dhcp snooping verify mac-address** command to leave the ports untrusted by disabling the MAC address verification on the client hardware address field.

Examples

This example shows how to verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port:

```
Router(config)# ip dhcp snooping verify mac-address
```

This example shows how to turn off the verification of the MAC address on the client hardware address field:

```
Router(config)# no ip dhcp snooping verify mac-address
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping vlan

To enable DHCP snooping on a VLAN or a group of VLANs, use the **ip dhcp snooping vlan** command in global configuration mode. To disable DHCP snooping on a VLAN or a group of VLANs, use the **no** form of this command.

ip dhcp snooping vlan {*number* | *vlan-list*}

no ip dhcp snooping vlan {*number* | *vlan-list*}

Syntax Description

number | *vlan-list*	VLAN number or a group of VLANs; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	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

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Enter the range of VLANs using this format: 1,3-5,7,9-11.

Examples

This example shows how to enable DHCP snooping on a VLAN:

```
Router(config)# ip dhcp snooping vlan 10
```

This example shows how to disable DHCP snooping on a VLAN:

```
Router(config)# no ip dhcp snooping vlan 10
```

This example shows how to enable DHCP snooping on a group of VLANs:

```
Router(config)# ip dhcp snooping vlan 10,4-8,55
```

This example shows how to disable DHCP snooping on a group of VLANs:

```
Router(config)# no ip dhcp snooping vlan 10,4-8,55
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp subscriber-id interface-name

To automatically generate a subscriber identifier (ID) value based on the short name of the interface, use the **ip dhcp subscriber-id interface-name** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp subscriber-id interface-name

no ip dhcp subscriber-id interface-name

Syntax Description

This command has no arguments or keywords.

Command Default

A subscriber ID is not automatically generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A subscriber ID configured on a specific interface using the **ip dhcp server use subscriber-id client-id** command takes precedence over the global configuration.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
ip dhcp server use subscriber-id client-id	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface.

ip dhcp use

To control what information the Dynamic Host Configuration Protocol (DHCP) server accepts or rejects during address allocation, use the **ip dhcp use** command in global configuration mode. To disable the use of these parameters during address allocation, use the **no** form of this command.

ip dhcp use {class | vrf {connected | remote}}

no ip dhcp use {class | vrf {connected | remote}}

Syntax Description

class	Specifies that the DHCP server use DHCP classes during address allocation.
vrf	Specifies whether the DHCP server ignores or uses the receiving VRF (VPN Routing and Forwarding) interface during address allocation.
connected	Specifies that the server should use the VRF information from the receiving interface when servicing a directly connected client.
remote	Specifies that the server should use the VRF information from the receiving interface when servicing a request forwarded by a relay agent.

Command Default

The DHCP server allocates addresses by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When the Cisco IOS DHCP server code is allocating addresses, you can use the **ip dhcp use** command to either enable or disable the use of VRF configured on the interface, or to configure DHCP classes. If you use the **no ip dhcp use class** command, the DHCP class configuration is not deleted.

Examples

The following example shows the DHCP server configured to use the relay agent information option during address allocation:

```
Router(config)# ip dhcp use class
```

The following example shows the DHCP server configured to disable the use of the VRF information option during address allocation:

```
Router(config)# no ip dhcp use vrf connected
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

ip dhcp use subscriber-id client-id

To configure the Dynamic Host Configuration Protocol (DHCP) server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages, use the **ip dhcp use subscriber-id client-id** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp use subscriber-id client-id

no ip dhcp use subscriber-id client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP uses the client identifier option in the DHCP packet to identify clients.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

A subscriber ID value configured on a specific interface using the **ip dhcp server use subscriber-id client-id** command takes precedence over this command.

Examples

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client identifier fields in the DHCP messages and use this subscriber ID as the client identifier. The DHCP client is preassigned IP address 10.1.1.7.

```
Router(config)# ip dhcp use subscriber-id client-id
Router(config)# ip dhcp subscriber-id interface-name
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.3
Router(config)# ip dhcp pool dhcppool
Router(dhcp-config)# network 10.1.1.0 255.255.255.0
Router(dhcp-config)# address 10.1.1.7 client-id ethernet 1/0 ascii
```

Related Commands

Command	Description
ip dhcp server use subscriber-id client id	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface.

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** command in DHCP pool configuration mode. To restore the default value, use the **no** form of this command.

lease {*days* [*hours* [*minutes*]] | **infinite**}

no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Defaults

1 day

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 shows a 1-day lease:

```
lease 1
```

The following example shows a 1-hour lease:

```
lease 0 1
```

The following example shows a 1-minute lease:

```
lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
lease infinite
```

Related Commands

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

netbios-name-server

To configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-name-server** command in DHCP pool configuration mode. To remove the NetBIOS name server list, use the **no** form of this command.

netbios-name-server *address* [*address2...address8*]

no netbios-name-server

Syntax Description

address	Specifies the IP address of the NetBIOS WINS name 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 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

One IP address is required, although you can specify up to eight addresses in one command line. 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 the IP address of a NetBIOS name server available to the client:

```
netbios-name-server 10.12.1.90
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
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.
netbios-node-type	Configures the NetBIOS node type for Microsoft DHCP clients.

netbios-node-type

To configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-node-type** command in DHCP pool configuration mode. To remove the NetBIOS node type, use the **no** form of this command.

netbios-node-type *type*

no netbios-node-type

Syntax Description

type	Specifies the NetBIOS node type. Valid types are: • **b-node**—Broadcast • **p-node**—Peer-to-peer • **m-node**—Mixed • **h-node**—Hybrid (recommended)

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 recommended type is h-node (hybrid).

Examples

The following example specifies the client's NetBIOS type as hybrid:

```
netbios node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios name-server	Configures NetBIOS WINS name servers that are available to Microsoft DHCP clients.

network (DHCP)

To configure the network number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool primary or secondary subnet on a Cisco IOS DHCP server, use the **network** command in DHCP pool configuration mode. To remove the subnet number and mask, use the **no** form of this command.

network *network-number* [*mask* [**secondary**] | /*prefix-length* [**secondary**]

no network *network-number* [*mask* [**secondary**] | /*prefix-length* [**secondary**]

Syntax Description

network-number	The IP address of the primary DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
/*prefix-length*	(Optional) 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 (/).
secondary	(Optional) The network address specifies a secondary subnet in the DHCP address pool, and the router enters DHCP pool secondary subnet configuration mode. **Note** To configure a secondary subnet, you must also specify the *mask* argument or the p*refix-length* argument.

Defaults

This command is disabled by default.

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.
12.2(33)SRB	This command was modified. The **secondary** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is valid for DHCP subnetwork address pools only.

The DHCP server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** global configuration command. However, the **ip dhcp excluded-address** command cannot be used to exclude addresses from virtual routing and forwarding (VRF)-associated pools.

You cannot configure manual bindings within the same pool that is configured with the **network** command.

If a default router list is configured for the pool or subnet from which the address was allocated, the DHCP server selects an IP address from that default router list and provides it to the client. The DHCP client uses that router as the first hop for forwarding messages.

Removing a secondary subnet also removes the default router list for that subnet. Removing the primary subnet removes only the primary subnet definition but not the network-wide default router list.

To display the DHCP address pool information configured by the **network** command, use the **show ip dhcp pool** command.

Examples

The following example shows how to configure 172.16.0.0/12 as the subnetwork number and mask of the DHCP pool named pool1. The IP addresses in pool1 range from 172.16.0.0 to 172.31.255.255.

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# network 172.16.0.0 255.240.0.0
```

The following example shows how to configure 192.0.2.0/24 as the subnetwork number and mask of the DHCP pool named pool2 and then add the DHCP pool secondary subnet specified by the subnet number and mask 192.0.4.0/30. The IP addresses in pool2 consist of two unconnected subnets: the addresses from 192.0.2.1 to 192.0.2.254 and the addresses from 192.0.4.1 to 192.0.4.2.

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
```

Related Commands

Command	Description
default-router	Specifies the IP address of the default router for a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
override default-router	Configures a subnet-specific default router list for the DHCP pool secondary subnet.
show ip dhcp pool	Displays information about the DHCP address pools.

next-server

To configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client, use the **next-server** command in DHCP pool configuration mode. To remove the boot server list, use the **no** form of this command.

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

no next-server *address*

Syntax Description

address	Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One IP address is required, but up to eight addresses can be specified in one command line.
address2...address8	(Optional) Specifies up to seven additional addresses in the command line.

Defaults

If the **next-server** command is not used to configure a boot server list, the DHCP server uses inbound interface helper addresses as boot servers.

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

You can specify up to eight servers in the list. 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 next server in the boot process:

```
next-server 10.12.1.99
```

Related Commands

Command	Description
accounting (DHCP)	Specifies the name of the default boot image for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
option	Configures Cisco IOS DHCP server options.

option

To configure Dynamic Host Configuration Protocol (DHCP) server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option *code* [**instance** *number*] {**ascii** *string* | **hex** {*string* | **none**} | **ip** *address*}

no option *code* [**instance** *number*]

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254.
instance *number*	(Optional) Specifies an instance number. The range is from 0 to 255. The default is 0.
ascii *string*	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
hex	Specifies dotted hexadecimal data.
string	Hexadecimal value. Each byte in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.
none	Specifies the zero length hexadecimal string.
ip *address*	Specifies the hostname or an IP address. More than one hostname or IP address can be specified with one CLI.

Defaults

The default instance number is 0.

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 was supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	This command was modified. The **none** keyword was added.

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding; a value of 1 means enable IP forwarding. IP forwarding is enabled in the following example:

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 19 hex 01
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 72 ip 172.16.3.252 172.16.3.253
```

Related Commands

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

option hex

To enable the Cisco IOS relay agent to make forwarding decisions based on DHCP options inserted in the client-generated DHCP message, use the **option hex** command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

option *code* **hex** *hex-pattern* [*] [**bit** *bit-mask-pattern*]

no option *code* **hex** *hex-pattern* [*] [**mask** *bit-mask-pattern*]

Syntax Description

code	Specifies the DHCP option code. Valid values are 60, 77, 124, and 125. All other values will be rejected with the appropriate error message.
hex-pattern	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class. The *hex-pattern* argument represents the data portion of the DHCP option format. See "Usage Guidelines" below for more information.
*	(Optional) Wildcard character.
mask *bit-mask-pattern*	(Optional) String of hexadecimal values. Specifies the bit mask to be applied to the *hex-pattern* argument.

Command Default

This command is disabled by default.

Command Modes

DHCP class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **option hex** command enhances DHCP class support to allow the relay agent to relay client-generated messages to different DHCP servers based on the content of the following four options:

- Option 60: vendor class identifier
- Option 77: user class
- Option 124: vendor-identifying vendor class
- Option 125: vendor-identifying vendor-specific information

Each option identifies the type of client sending the DHCP message.

Table 9 describes the CLI variations possible for the **hex** *hex-pattern* keyword and argument combination.

Table 9 option hex CLI Variations

Hex string format variations	CLI example	Description
Full option value as raw hex	`option 60 hex 010203`	This option has 3 bytes of data with 0x010203 hex as the content.
Bit-masked hex string	`option 60 hex 010203 mask 0000FF`	This option is the same as above except that only the first 2 bytes of data should be 0x0102.
Wild-carded hex string	`option 60 hex 010203*`	This option should have at least 3 bytes, with the first 3 bytes matching the specified hex pattern.

You must know the hexadecimal value of each byte location in the options to be able to configure the **option hex** command. The format may vary from product to product. Contact the relay agent vendor for this information.

Examples

In the following example, client-generated DHCP messages containing option 60 and belonging to class VOIP will be forwarded to the DHCP server located at 10.30.5.1:

```
!
ip dhcp class VOIP
 option 60 hex 010203
!
! The following is the relay pool
ip dhcp pool red
 relay source 10.2.2.0 255.255.255.0
 class VOIP
  relay target 10.30.5.1
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class configuration mode.

origin

To configure an address pool as an on-demand address pool (ODAP) or static mapping pool, use the **origin** command in DHCP pool configuration mode. To disable the ODAP, use the **no** form of this command.

origin {**dhcp** | **aaa** | **ipcp** | **file** *url*} [**subnet size initial** *size* [**autogrow** *size*]]

no origin {**dhcp** | **aaa** | **ipcp** | **file** *url*} [**subnet size initial** *size* [**autogrow** *size*]]

Syntax Description

dhcp	Specifies the Dynamic Host Configuration Protocol (DHCP) as the subnet allocation protocol.
aaa	Specifies authentication, authorization, and accounting (AAA) as the subnet allocation protocol.
ipcp	Specifies the IP Control Protocol (IPCP) as the subnet allocation protocol.
file *url*	Specifies the external database file that contains the static bindings assigned by the DHCP server. The *url* argument specifies the location of the external database file.
subnet size initial *size*	(Optional) Specifies the initial size of the first requested subnet. You can enter *size* as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
autogrow *size*	(Optional) Specifies that the pool can grow incrementally. The *size* argument is the size of the requested subnets when the pool requests additional subnets (upon detection of high utilization). You can enter *size* as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.

Defaults

The default size value is /0.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(11)T	The **file** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool.

Use the **dhcp** keyword to obtain subnets from DHCP, the **aaa** keyword to obtain subnets from the AAA server, and the **ipcp** keyword to obtain subnets from IPCP negotiation. If you expect that the utilization of the pool may grow over time, use the **autogrow** *size* option.

If a pool has been configured with the **autogrow** *size* option, ensure that the source server is capable of providing more than one subnet to the same pool. Even though the Cisco IOS software specifies the requested subnet size, it can accept any offered subnet size from the source server.

Examples

The following example shows how to configure an address pool named green to use DHCP as the subnet allocation protocol with an initial subnet size of 24 and an autogrow subnet size of 24:

```
ip dhcp pool pool1
  vrf pool1
  origin dhcp subnet size initial /24 autogrow /24
  utilization mark high 80
  utilization mark low 20
```

The following example shows how to configure the location of the external text file:

```
ip dhcp pool abcpool
 origin file tftp://10.1.0.1/staticbindingfile
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

override default-router

To define a default router list for the DHCP pool secondary subnet, use the **override default-router** command in DHCP pool secondary subnet configuration mode. To remove the default router list for this secondary subnet, use the **no** form of this command.

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

no override default-router

Syntax Description

address	IP address of the default router for the DHCP pool secondary subnet, preferably on the same subnet as the DHCP pool secondary client subnet.
address2 ... address8	(Optional) IP addresses of up to seven additional default routers, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering IP addresses.

Command Default

No default router list is defined for the DHCP pool secondary subnet.

Command Modes

DHCP pool secondary subnet configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

When an IP address is assigned to the DHCP client from a secondary subnet for which no subnet-specific default router list is defined, the default router list (configured by using the **default-router** command in DHCP pool configuration mode) will be used.

The IP address of every router in the list 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 (*address* is the most preferred router, *address2* is the next most preferred router, and so on).

To display the default router lists, use the **show running-config** command. If default router lists are configured for a DHCP pool, the commands used to configure those lists are displayed following the **ip dhcp pool** command that configures the DHCP pool.

Examples

The following example configures 10.1.1.1/29 as the subnetwork number and mask of the DHCP pool named pool1, adds the DHCP pool secondary subnet specified by the subnet number and mask 10.1.1.17/29, then configures a subnet-specific default router list for that subnet:

```
Router(config)# dhcp pool pool1
Router(config-dhcp)# network 10.1.1.1 255.255.255.248
Router(config-dhcp)# network 10.1.1.17 255.255.255.248 secondary
Router(config-dhcp-secondary-subnet)# override default-router 10.1.1.100 10.1.1.200
```

Related Commands

Command	Description
default-router	Specifies the default router list for a DHCP client.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server.

override utilization high

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

override utilization high *percentage-number*

no override utilization high *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100 percent.

Command Default

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

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

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

Usage Guidelines

If you use the **utilization mark** {**high** | **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization exceeds the configured high utilization threshold. A system message can also be generated when the subnet's utilization is detected to be below the configured low utilization threshold.

The **override utilization high** command overrides the value specified by the **utilization mark high** global configuration command.

Examples

The following example shows how to set the high utilization mark of the secondary subnet to 40 percent of the current subnet size:

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

Related Commands

Command	Descriptions
override utilization low	Configures the low utilization mark of the current subnet size.
utilization mark high	Configures the high utilization mark of the current address pool size.

override utilization low

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

override utilization low *percentage-number*

no override utilization low *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100.

Command Default

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

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

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

Usage Guidelines

If you use the **utilization mark** {**high** | **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization falls below the configured low utilization threshold. A system message can also be generated when the subnet's utilization exceeds the configured high utilization threshold.

The **override utilization low** command overrides the value specified by the **utilization mark low** global configuration command.

Examples

The following example shows how to set the low utilization mark of the secondary subnet to 30 percent of the current subnet size:

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

Related Commands

Command	Description
override utilization high	Configures the high utilization mark of the current subnet size.
utilization mark low	Configures the low utilization mark of the current address pool size.

rbe nasip

To specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove the specification, use the **no** form of this command.

rbe nasip *interface-type number*

no rbe nasip

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

No IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

The **rbe nasip** command is used to configure support for the DHCP relay agent information option (option 82) for an ATM routed bridge encapsulation (RBE).

Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the **ip dhcp relay information option** command for the **rbe nasip** command to be effective.

Examples

The following example shows how to enable support for DHCP option 82 on the DHCP relay agent by using the **ip dhcp relay agent information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM routed bridge encapsulation is configured on ATM subinterface 4/0.1.

```
ip dhcp-server 10.1.1.1
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM 4/0
 no ip address
```

```
!
interface ATM 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.1.1.1
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
router eigrp 100
 network 10.0.0.0
!
rbe nasip loopback0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

relay agent information

To enter relay agent information option configuration mode, use the **relay agent information** command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

relay agent information

no relay agent information

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

DHCP class configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If this command is omitted for Dynamic Host Configuration Protocol (DHCP) class-based address allocation, then the DHCP class matches to any relay agent information option, whether it is present or not.

Using the **no relay agent information** command removes all patterns in the DHCP class configured by the **relay-information hex** command.

Examples

The following example shows the relay information patterns configured for DHCP class 1.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
 relay agent information
```

Related Commands

Command	Description
relay-information hex	Specifies a hexadecimal string for the full relay agent information option.

relay destination

To configure an IP address for a relay destination to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) relay agent functioning as a DHCP server, use the **relay destination** command in DHCP pool configuration mode. To disable the IP address, use the **no** form of this command.

relay destination [**vrf** *vrf-name* | **global**] *ip-address*

no relay destination [**vrf** *vrf-name* | **global**] *ip-address*

Syntax Description

vrf	(Optional) Virtual routing and forwarding (VRF) instance that is associated with the relay destination address. The *vrf-name* argument specifies the name of the VRF table.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Defaults

No destination IP address to which packets are forwarded is configured.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **relay destination** command serves the same function as the **relay target** command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the service gateway (SG).

When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.

relay-information hex

To specify a hexadecimal string for the full relay agent information option, use the **relay-information hex** command in relay agent information option configuration mode. To remove the configuration, use the **no** form of this command.

relay-information hex *pattern* [*] [**bitmask** *mask*]

no relay-information hex *pattern* [*] [**bitmask** *mask*]

Syntax Description

pattern	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class.
*****	(Optional) Wildcard character.
bitmask *mask*	(Optional) Hexadecimal bitmask.

Defaults

No default behavior or values

Command Modes

Relay agent information option configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **relay-information hex** command sets a pattern that is used to match against defined DHCP classes. You can configure multiple **relay-information hex** commands for a DHCP class. This is useful to specify a set of relay information options that can not be summarized with a wildcard or a bitmask.

The pattern itself, excluding the wildcard, must contain a whole number of bytes (a byte is two hexadecimal numbers). For example, 010203 is 3 bytes (accepted) and 01020 is 2.5 bytes (not accepted).

If you omit this command, no pattern is configured and it is considered a match to any relay agent information value, but the relay information option must be present in the DHCP packet.

You must know the hexadecimal value of each byte location in option 82 to be able to configure the **relay- information hex** command. The option 82 format may vary from product to product. Contact the relay agent vendor for this information.

Examples

The following example shows the configured relay agent information patterns. Note that CLASS 2 has no pattern configured and will “match to any” class.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
 relay agent information
```

relay source

To configure an IP address for a relay source from which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay source** command in DHCP-pool configuration mode. To disable the IP address, use the **no** form of this command.

relay source *ip-address subnet-mask*

no relay source *ip-address subnet-mask*

Syntax Description

ip-address	IPv4 address of DHCP server from which the DHCP client packets are relayed.
subnet-mask	Subnet mask that matches the subnet of the incoming interface of the DHCP client packet.

Defaults

No IP address from which IP packets are forwarded is configured.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows how to configure a source IP address from which DHCP client packets are relayed:

```
ip dhcp pool abc1
 relay source 10.0.0.0 255.255.0.0
 relay destination 10.5.1.1
```

Related Commands

Command	Description
relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
relay target	Configures an IP address for a relay target to which packets are forward by a DHCP server.

relay target

To configure an IP address for a relay target to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay target** command in DHCP pool class configuration mode. To disable the IP address, use the **no** form of this command.

relay target [**vrf** *vrf-name* | **global**] *ip-address*

no relay target [**vrf** *vrf-name* | **global**] *ip-address*

Syntax Description

vrf	(Optional) Configured virtual routing and forwarding (VRF) that is associated with the relay destination address. The *vrf-name* argument specifies the name of the VRF table. **Note** If the **vrf** keyword is not specified, the target address is assumed to be in the same address space as the DHCP pool. If the **vrf** keyword is specified, the same VRF is assumed to apply here. However, if the target IP address is actually in the global address space, the **global** keyword should be specified.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Defaults

No target IP address is configured.

Command Modes

DHCP pool class configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **relay target** command serves the same function as the **relay destination** command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the SG.

Examples

The following example shows how to configure a relay target if a service gateway (SG)-supplied class name is used to select a DHCP server to which packets are relayed:

```
ip dhcp pool abc1
 relay source 10.0.0. 255.255.0.0.
 relay destination 10.5.1.1
 class classname1
  relay target 10.1.1.1
 class classname2
  relay target 10.2.2.2
 class classname3
```

In the above example, classname1 relays the DHCP DISCOVER packet to the server at 10.1.1.1, while classname2 relays the DHCP DISCOVER packet to the server at 10.2.2.2.

If the SG returned classname3, then the default pool at 10.5.1.1 is used. If the SG returns any other class name other than classname1, classname2, or classname3, then no relay action is taken.

The relay target configuration with respect to any configured DHCP pool works in the exact same way as a relay destination configuration works.

Related Commands

Command	Description
relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
relay source	Configures an IP address for a relay source from which packets are forward by a DHCP server.

release dhcp

To perform an immediate release of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **release dhcp** command in user EXEC or privileged EXEC mode.

release dhcp *interface-type interface-number*

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **release dhcp** command immediately releases the DHCP lease on the interface specified by the *interface-type* and *interface-number* arguments. If the router interface was not assigned a DHCP IP address by the DHCP server, the **release dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples

The following example shows how to release a DHCP lease for an interface.

```
release dhcp ethernet 3/1
```

Related Commands

Command	Description
ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
renew dhcp	Forces the renewal of the DHCP lease for the specified interface.
show dhcp lease	Displays the DHCP addresses leased from a server.
show interface	Displays statistics for all interfaces configured on the router or access server.

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface's IP information and status.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.

renew deny unknown

To configure the renewal policy for unknown DHCP clients, use the **renew deny unknown** command in DHCP pool configuration mode. To disable the renewal policy, use the no form of this command.

renew deny unknown

no renew deny unknown

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP server ignores a client request for an IP address that is not leased to the client.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2 SXH	This command was integrated into 12.2 SXH.

Usage Guidelines

In some usage scenarios, such as a wireless hotspot, where both DHCP and secure ARP are configured, a connected client device might go to sleep or suspend for a period of time. If the suspended time period is greater than the secure ARP timeout (default of 91 seconds), but less than the DHCP lease time, the client can awake with a valid lease, but the secure ARP timeout has caused the lease binding to be removed because the client has been inactive. When the client awakes, the client still has a lease on the client side but is blocked from sending traffic. The client will try to renew its IP address but the DHCP server will ignore the request because the DHCP server has no lease for the client. The client must wait for the lease to expire before being able to recover and send traffic again.

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

Examples

The following example shows how to secure ARP table entries to DHCP leases. The **renew deny unknown** command allows the DHCP server to renew the lease of a DHCP client whose lease has been cleared because of a secure ARP timeout.

```
Router# configure terminal
Router(config)# ip dhcp pool red
Router(dhcp-config)# update arp
Router(dhcp-config)# renew deny unknown
```

Related Commands

Command	Description
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

renew dhcp

To perform an immediate renewal of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **renew dhcp** command in user EXEC or privileged EXEC mode.

renew dhcp *interface-type interface-number*

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **renew dhcp** command immediately renews the DHCP lease for the interface specified by the *interface-type* and *interface-number* arguments. If the router interface was not assigned an IP address by the DHCP server, the **renew dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples

The following example shows how to renew a DHCP lease for an interface:

```
renew dhcp Ethernet 3/1
```

Related Commands

Command	Description
ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
release dhcp	Releases the DHCP lease on the specified interface.
show dhcp lease	Displays the DHCP addresses leased from a server.
show interface	Displays statistics for all interfaces configured on the router or access server.

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface’s IP information and status.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.

reserved-only

To restrict address assignments from the Dynamic Host Configuration Protocol (DHCP) address pool only to the preconfigured reservations, use the **reserved-only** command in DHCP pool configuration mode. To disable the configuration, use the **no** form of this command.

reserved-only

no reserved-only

Syntax Description

This command has no arguments or keywords.

Command Default

Address assignments from the DHCP address pool are not restricted only to the preconfigured reservations.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(50)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

When the DHCP port-based assignment feature is configured on multiple switches, devices connected to one switch may receive an IP address assignment from the neighboring switches rather than from the local DHCP address pool switch. If you want the switch to serve only the client directly connected to the switch, you can configure a group of switches with pools that share a common IP subnet but ignore the requests from other clients (not connected to this switch).

Examples

The following example shows how to restrict address assignments from the DHCP address pool only to the preconfigured reservations:

```
Router# configure terminal
Router(config)# ip dhcp pool red
Router(dhcp-config)# reserved-only
```

Related Commands

Command	Description
address client-id	Reserves an IP address for a DHCP client identified by client identifier.
address hardware-address	Reserves an IP address for a client identified by hardware address.

service dhcp

To enable the Dynamic Host Configuration Protocol (DHCP) server and relay agent features on your router, use the **service dhcp** command in global configuration mode. To disable the DHCP server and relay agent features, use the **no** form of this command.

service dhcp

no service dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

DHCP is enabled.
DHCP is not running.
Port 67 is closed.

Command Modes

Global configuration (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.
12.4	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.
12.2SXH	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.

Usage Guidelines

The BOOTP and DHCP servers in Cisco IOS software both use the Internet Control Message Protocol (ICMP) port (port 67) by default. ICMP “port unreachable messages” will only be returned to the sender if both the BOOTP server and DHCP server are disabled. Disabling only one of the servers will not result in ICMP port unreachable messages.

Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 is not opened until the DHCP service is running. A DHCP address pool must be configured for the DHCP service to be running. If the service is running, the s**how ip sockets detail** or **show sockets detail** commands displays port 67 as open.

Examples

The following example shows to enable DHCP services on the DHCP server:

```
service dhcp
```

Related Commands

Command	Description
show ip sockets	Displays IP socket information.
show sockets	Displays IP socket information.

set ip next-hop dynamic dhcp

To set the next hop to the gateway that was most recently learned by the Dynamic Host Configuration Protocol (DHCP) client, use the **set ip next-hop dynamic dhcp** command in route-map configuration mode. To restore the default setting, use the **no** form of this command.

set ip next-hop dynamic dhcp

no set ip next-hop dynamic dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **set ip next-hop dynamic dhcp** command supports only a single DHCP interface. If multiple interfaces have DHCP configured, the gateway that was most recently learned among all interfaces running DHCP will be used by the route map.

Examples

The following example configures a local routing policy that sets the next hop to the gateway that was most recently learned by the DHCP client:

```
access list 101 permit icmp any host 172.16.23.7 echo
route map MY-LOCAL-POLICY permit 10
 match ip address 101
 set ip next-hop dynamic dhcp
!
ip local policy route-map MY-LOCAL-POLICY
```

Related Commands

Command	Description
access list (IP extended)	Defines an extended IP access list.

show ip dhcp binding

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** command in user EXEC or privileged EXEC mode.

Cisco IOS Release 12.0(1)T, 12.2(28)SB, and Later Releases

show ip dhcp binding [*ip-address*]

Cisco IOS Release 12.2(33)SRC and Later 12.2SR Releases

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

Syntax Description

ip-address	(Optional) IP address of the DHCP client for which bindings will be displayed. If the *ip-address* argument is used with the **vrf** *vrf-name* option, the binding in the specified VPN routing and forwarding (VRF) instance is displayed.
vrf *vrf-name*	(Optional) Specifies the name of a VRF instance.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(15)T	The command was modified. Support to display allocated subnets was added to the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SB9	This command was modified. The output was modified to display the option 82 suboptions of the remote ID and circuit ID.

Usage Guidelines

This command is used to display DHCP binding information for IP address assignment and subnet allocation. If a specific IP address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address display only an IP address and are not followed by a subnet mask.

Examples

IP Address Assignment Example

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, the type of address assignment that has occurred, and the option 82 suboptions of the remote ID and circuit ID.

Table 10 describes the significant fields shown in the displays.

```
Router# show ip dhcp binding 192.0.2.2

IP address          Client-ID/             Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           aabb.cc00.0a00         Apr 28 2010 05:00 AM    Automatic
Remote id : 020a0000140006400000000
```

Table 10 show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Client-ID/Hardware address/User name	The MAC address or client ID of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.
Remote id	Information sent to the DHCP server using a suboption of the remote ID.

Subnet Allocation Example

The following example shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default):

```
Router# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/             Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2/24        0063.6973.636f.2d64.   Mar 29 2003 04:36 AM    Automatic
                    656d.6574.6572.2d47.
                    4c4f.4241.4c
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server. The subnet that follows the IP address (/26) in the example defines this binding as a subnet allocation binding.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
show ip dhcp vrf	Displays VRF information on the DHCP server.

show ip dhcp conflict

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

show ip dhcp conflict [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Displays virtual routing and forwarding (VRF) address conflicts found by the DHCP server.
vrf-name	(Optional) The VRF name.

Command Default

If you do not enter the IP address or VRF then all dhcp conflict related information is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

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.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The server uses a ping operation to detect conflicts. The client uses gratuitous Address Resolution Protocol (ARP) to detect clients. If an address conflict is detected, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.

Examples

The following is sample output from the show ip dhcp conflict command, which shows the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices:

```
Router# show ip dhcp conflict

IP address     Detection method     Detection time         VRF
172.16.1.32    Ping                 Feb 16 1998 12:28 PM   vrf1
172.16.1.64    Gratuitous ARP       Feb 23 1998 08:12 AM   vrf2
```

Table 12 describes the fields shown in the display.

Table 12 show ip dhcp conflict Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection method	The manner in which the IP address of the hosts were found on the DHCP server. Can be a ping or a gratuitous ARP.
Detection time	The date and time when the conflict was found.
VRF	VRFs configured on the DHCP server.

The following is sample output from the **show ip dhcp conflict vrf** command:

```
Router# show ip dhcp conflict vrf vrf1

IP address        Detection method   Detection time         VRF
172.16.1.32       Ping               Feb 15 2009 05:39 AM    vrf1
```

See Table 12 for the field description.

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping packets	Specifies the number of packets a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.

show ip dhcp database

To display Dynamic Host Configuration Protocol (DHCP) server database agent information, use the **show ip dhcp database** command in privileged EXEC mode.

show ip dhcp database [*url*]

Syntax Description

url	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename

Defaults

If a URL is not specified, all database agent records are shown. Otherwise, only information about the specified agent is displayed.

Command Modes

Privileged EXEC

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 shows all DHCP server database agent information. Table 13 describes the significant fields shown in the display.

```
Router# show ip dhcp database

URL       :    ftp://user:password@172.16.4.253/router-dhcp
Read      :    Dec 01 1997 12:01 AM
Written   :    Never
Status    :    Last read succeeded. Bindings have been loaded in RAM.
Delay     :    300 seconds
Timeout   :    300 seconds
Failures  :    0
Successes :    1
```

Table 13 show ip dhcp database Field Descriptions

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
Read	The last date and time bindings were read from the file server.
Written	The last date and time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time (in seconds) to wait before updating the database.
Timeout	The amount of time (in seconds) before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

Related Commands

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

show ip dhcp import

To display the option parameters that were imported into the Dynamic Host Configuration Protocol (DHCP) server database, use the **show ip dhcp import** command in privileged EXEC command.

show ip dhcp import

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

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

Imported option parameters are not part of the router configuration and are not saved in NVRAM. Thus, the **show ip dhcp import** command is necessary to display the imported option parameters.

Examples

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

```
Router# show ip dhcp import

Address Pool Name:2
Domain Name Server(s): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

The following example indicates the address pool name:

```
Address Pool Name:2
```

The following example indicates the imported values, which are domain name and NetBIOS name information:

```
Domain Name Server(s): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

Related Commands

Command	Description
import all	Imports option parameters into the DHCP database.
show ip dhcp database	Displays Cisco IOS server database information.

show ip dhcp limit lease

To display the number of times the lease limit threshold has been violated, use the **show ip dhcp limit lease** command in user EXEC or privileged EXEC mode.

show ip dhcp limit lease [*type number*]

Syntax Description

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 system for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

You can control the number of subscribers at the global level by using the **ip dhcp limit lease per interface** command and at the interface level by using the **ip dhcp limit lease** command. The **show ip dhcp limit lease** command displays the number of lease limit violations per interface or at the global level.

Examples

In the following example, the number of lease violations is displayed. If the **ip dhcp limit lease log** command is enabled, the show output will indicate that lease limit logging is enabled:

```
Router# show ip dhcp limit lease

DHCP limit lease logging is enabled
Interface        Count
Serial0/0.1      5
Serial1          3
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.
ip dhcp limit lease log	Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded.
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

show ip dhcp pool

To display information about the Dynamic Host Configuration Protocol (DHCP) address pools, use the **show ip dhcp pool** command in user EXEC or privileged EXEC mode.

show ip dhcp pool [*name*]

Syntax Description

name	(Optional) Name of the address pool.

Command Default

If a pool name is not specified, information about all address pools is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was modified. The command output was enhanced to display information about excluded addresses in network pools.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use this command to determine the subnets allocated and to examine the current utilization level for the pool or all the pools if the *name* argument is not used.

Examples

The following example shows DHCP address pool information for an on-demand address pool (ODAP), pool 1. Table 14 describes the significant fields shown in the display.

```
Router# show ip dhcp pool 1

Pool 1:
 Utilization mark (high/low)    : 85 / 15
 Subnet size (first/next)       : 24 / 24 (autogrow)
 VRF name                       : abc
 Total addresses                : 28
 Leased addresses               : 11
 Pending event                  : none
 2 subnets are currently in the pool :
 Current index        IP address range           Leased addresses
 10.1.1.12            10.1.1.1 - 10.1.1.14       11
 10.1.1.17            10.1.1.17 - 10.1.1.30      0
 Interface Ethernet0/0 address assignment
   10.1.1.1 255.255.255.248
   10.1.1.17 255.255.255.248 secondary
```

The following example shows DHCP address pool information for a network pool, pool 2. Table 14 describes the significant fields shown in the display.

```
Router# show ip dhcp pool 2

Pool pool2 :
Utilization mark (high/low) : 80 / 70
Subnet size (first/next) : 0 / 0
Total addresses : 256
Leased addresses : 0
Excluded addresses : 2
Pending event : none
2 subnets are currently in the pool:
Current index    IP address range         Leased/Excluded/Total
10.0.2.1         10.0.2.1 - 10.0.2.254     0      / 1      / 254
10.0.4.1         10.0.4.1 - 10.0.4.2       0      / 1      / 2
```

Table 14 show ip dhcp pool Field Descriptions

Field	Description
Pool	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.
Total addresses	The total number of addresses in the pool.
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.
Excluded addresses	The number of excluded addresses.
Interface Ethernet0/0 address assignment	The first line is the primary IP address of the interface. The second line is the secondary IP address of the interface. More than one secondary address on the interface is supported.

Related Commands

Command	Description
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode.
ip dhcp subscriber-id interface-name	Automatically generates a subscriber ID value based on the short name of the interface.
ip dhcp use subscriber-id client-id	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.

show ip dhcp relay information trusted-sources

To display all interfaces configured to be a trusted source for the Dynamic Host Configuration Protocol (DHCP) relay information option, use the **show ip dhcp relay information trusted-sources** command in user EXEC or privileged EXEC mode.

show ip dhcp relay information trusted-sources

Syntax Description

This command has no arguments or keywords.

Command Modes

user EXEC
privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(14)SX	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 not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

The following is sample output when the **ip dhcp relay information trusted-sources** command is configured. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Router# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
Ethernet1/1       Ethernet1/2       Ethernet1/3       Serial4/1.1
Serial4/1.2       Serial4/1.3
```

The following is sample output when the **ip dhcp relay information trust-all** global configuration command is configured. Note that the display output does not list the individual interfaces.

```
Router# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option Serial4/1.1
```

Related Commands

Command	Description
ip dhcp relay information trusted	Configures an interface as a trusted source of the DHCP relay agent information option.
ip dhcp relay information trust-all	Configures all interfaces on a router as trusted sources of the DHCP relay agent information option.

show ip dhcp server statistics

To display Dynamic Host Configuration Protocol (DHCP) server statistics, use the **show ip dhcp server statistics** command in privileged EXEC mode.

show ip dhcp server statistics

Syntax in Cisco IOS Release 12.2(33)SRC and Subsequent 12.2SR Releases

show ip dhcp server statistics [*type number*]

Syntax Description

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 system for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC

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.
12.2(33)SRC	The *type* and *number* arguments were added. The command was enhanced to display interface level DHCP statistics.

Examples

The following example displays DHCP server statistics. Table 15 describes the significant fields in the display.

```
Router# show ip dhcp server statistics

Memory usage          40392
Address pools         3
Database agents       1
Automatic bindings    190
Manual bindings       1
Expired bindings      3
Malformed messages    0
Secure arp entries    1
Renew messages        0

Message               Received
BOOTREQUEST           12
DHCPDISCOVER          200
DHCPREQUEST           178
DHCPDECLINE           0
```

```
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            12
DHCPOFFER            190
DHCPACK              172
DHCPNAK              6
```

Table 15 show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Secure arp entries	The number of ARP entries that have been secured to the MAC address of the client interface.
Renew messages	The number of renew messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP server counters.

show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command in privileged EXEC mode.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to display the DHCP snooping configuration:

```
Router# show ip dhcp snooping

Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 10
Insertion of option 82 is enabled
Interface               Trusted     Rate limit (pps)
--------------------    -------     ----------------
FastEthernet6/11        no          10
FastEthernet6/36        yes         50
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.

Command	Description
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping binding

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding** command in privileged EXEC mode.

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan*]
[**interface** *type number*]

Syntax Description

ip-address	(Optional) IP address for the binding entries.
mac-address	(Optional) MAC address for the binding entries.
vlan *vlan*	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.
interface *type*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
number	Module and port number.

Command Default

If no argument is specified, the switch displays the entire DHCP snooping binding table.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Router# show ip dhcp snooping binding

MacAddress      IP Address   Lease(seconds)  Type           VLAN   Interface
-----------     -----------  --------------  -------------  -----  --------------
0000.0100.0201  10.0.0.1     600             dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 172.16.101.102

MacAddress      IP Address      Lease (seconds)  Type           VLAN   Interface
-----------     -----------     ---------------  -------------  -----  ------------
0000.0100.0201  172.16.101.102  1600             dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f

MacAddress          IpAddress  Lease(sec)  Type           VLAN  Interface
------------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F   10.5.5.2   492         dhcp-snooping  99    FastEthernet6/36 Router#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f vlan 99

MacAddress         IpAddress  Lease(sec)  Type           VLAN  Interface
-----------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F  10.5.5.2   479         dhcp-snooping  99    FastEthernet6/36
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Router# show ip dhcp snooping binding vlan 100

MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
--------------     ----------  --------------  -------------  ----  --------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

This example shows how to display the DHCP snooping binding entries on Fast Ethernet interface 3/1:

```
Router# show ip dhcp snooping binding interface fastethernet3/1

MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
--------------     ----------  --------------  -------------  ----  --------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

Table 16 describes the fields in the **show ip dhcp snooping** command output.

Table 16 show ip dhcp snooping Command Output

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

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.

Command	Description
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database** command in privileged EXEC mode.

show ip dhcp snooping database [**detail**]

Syntax Description

detail	(Optional) Provides additional operating state and statistics information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	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.

Examples

This example shows how to display the DHCP snooping database:

```
Router# show ip dhcp snooping database

Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

This example shows how to view additional operating statistics:

```
Router# show ip dhcp snooping database detail

Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
```

```
Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

show ip dhcp vrf

To display the VPN routing and forwarding (VRF) instance information on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp vrf** command in user EXEC or privileged EXEC mode.

show ip dhcp vrf *vrf-name* **binding** {*ip-address* | *****}

Syntax Description

vrf-name	Specifies the VRF name.
binding	Displays DHCP VRF bindings.
ip-address	Specifies the IP address of the DHCP client for which bindings will be displayed.
*****	Displays all bindings in the specified VRF instance.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

This command is used to display VRF information on the Cisco IOS DHCP server. If an IP address is specified, VRF information for the specific client is displayed. If an asterisk (*) is specified, then VRF information for all the clients is displayed.

Examples

The following example shows the bindings associated with the VRF instance named red:

```
Router# show ip dhcp vrf red binding *

Bindings from VRF pool red:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.0           0063.6973.636f.2d30.    Mar 11 2007 04:36 AM    Automatic
                    3030.312e.3030.3131.
                    2e30.3032.342d.4574.
                    302f.30
192.0.2.1           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
                    3032.322e.3030.3333.
                    2e30.3034.342d.4574.
                    302f.30
```

The following example shows the bindings associated with a specific IP address in the VRF instance named red:

```
Router# show ip dhcp vrf red binding 192.0.2.2

IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
                    3032.322e.3030.3333.
                    2e30.3034.342d.4574.
                    302f.30
```

Table 17 describes the significant fields shown in the displays.

Table 17 show ip dhcp vrf Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

show ip route dhcp

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ip route dhcp

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

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

```
Router# show ip route dhcp 10.5.5.217

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

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

```
Router# show ip route vrf abc dhcp

  10.5.5.218/32 is directly connected, ATM0.2
```

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

```
Router# show ip route vrf red dhcp 10.5.5.218

  10.5.5.218/32 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

Related Commands

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

snmp-server enable traps dhcp

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

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

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

Syntax Description

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

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

subnet prefix-length

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

subnet prefix-length *prefix-length*

no subnet prefix-length *prefix-length*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

Configuring Global Subnet Pools

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

Configuring VPN Subnet Pools

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

Configuring VPN Subnet Pools for VPN clients with VPN IDs

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

Examples

Global Configuration Example

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

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

VPN Configuration Example

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

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

VPN ID Configuration Example

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

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

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
ip dhcp pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
show ip dhcp pool	Displays information about the DHCP pools.

update arp

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

update arp

no update arp

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

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

This command can be configured only under the following conditions:

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

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

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

Examples

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

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

Related Commands

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

utilization mark high

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

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

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

Syntax Description

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

Defaults

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

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(4)T	The **log** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

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

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

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

Examples

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

```
utilization mark high 80
```

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

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

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

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

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

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

Related Commands

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

utilization mark low

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

utilization mark low *percentage-number*

no utilization mark low *percentage-number*

Syntax Description

percentage-number	Percentage of the current pool size.

Defaults

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

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

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

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

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

Examples

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

```
utilization mark low 20
```

Related Commands

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

vrf (DHCP pool)

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

vrf *name*

no vrf *name*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

Examples

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

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

Related Commands

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

DNS Commands

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.

Defaults

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.

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.

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 router uses any configured domain name server addresses.

If there are no domain name server addresses configured either, the router 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 routers.

Command Modes

DNS view configuration

Command History

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

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).

Versions of Cisco IOS prior to Release 12.4(9)T used the resolving name server list for both 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:

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

```
Router(config)# ip dns view vrf vpn32 user1
Router(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.
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.
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.

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.
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-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 *name-server-ip-address*

no domain name-server *name-server-ip-address*

Syntax Description

name-server-ip-address	IP address of a 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 router 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.

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 router 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:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain name-server 192.168.2.111
Router(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 router 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.

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.

Defaults

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
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.

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* argument takes 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.

Defaults

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:

DDNS

```
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.
```

TZO

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

EASYDNS

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

JUSTLINUX

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

DYNS

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

HN

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

ZONEEDIT

```
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.
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.

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.

Defaults

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.

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.

Defaults

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

ip ddns update hostname

To enable a host to be used for Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **ip ddns update hostname** command in interface configuration mode. To disable the dynamic updates, use the **no** form of this command.

ip ddns update hostname *hostname*

no ip ddns update hostname *hostname*

Syntax Description

hostname	Specifies a hostname of the server that will receive updates. **Note** It is expected that the hostname will be an fully qualified domain name (FQDN). Using an FQDN hostname enables the specification of a hostname in a different domain that the default domain of the device.

Defaults

No host is configured.

Command Modes

Interface 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

The interface configuration overrides the global configuration.

Examples

The following example shows how to configure the testhost host to update A and PTR RRs:

```
interface ethernet1/0
 ip ddns update hostname testhost
```

Related Commands

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

ip ddns update method

To specify a method and method name for updating Dynamic Domain Name System (DDNS) address (A) and pointer (PTR) Resource Records (RRs) and enter DDNS-update-method configuration mode, use the **ip ddns update method** command in global configuration mode. To disable the dynamic updating, use the **no** form of this command.

ip ddns update method *method-name*

no ip ddns update method

Syntax Description

method-name	IETF standardized DDNS update method name.

Defaults

No DDNS update method is configured.

Command Modes

Global 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

The interface configuration overrides the global configuration.

Examples

The following example shows how to assign a DDNS update method name:

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

Once you have assigned the method name, you can specify the type of update (DDNS or HTTP) and set a maximum interval. Refer to the **ddns** and **http** commands for more information.

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
http	Specifies HTTP as the update method for A and PTR RRs.

ip dhcp client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp client update dns** command in interface configuration mode. To disable dynamic updates of A RRs, use the **no** form of this command.

ip dhcp client update dns [**server** {**both** | **none**}]

no ip dhcp client update dns [**server** {**both** | **none**}]

Syntax Description

server	(Optional) Specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this configuration and do the updates anyway. • **both**—Enables the DHCP client to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously. **Note** If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This keyword instructs the server that it should attempt to dynamically update both the A and PTR RRs. • **none**—On the client side, specifies that the DHCP client should include the FQDN option; however, it should not attempt any DDNS updates. **Note** If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Defaults

No default behavior.

Command Modes

Interface 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

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp-client update dns** command (hyphenated) is the global configuration command.

If you specify the **both** and **none** keywords in separate configurations, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference to what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

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

Examples

The following example shows how to configure the DHCP client to perform A and PTR RR updates, but the DHCP server will not perform the updates:

```
ip dhcp client update dns server none
```

Related Commands

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

ip dhcp-client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp-client update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

ip dhcp-client update dns [**server** {**both** | **none**}]

no ip dhcp client update dns

Syntax Description

server — (Optional) Enables the Dynamic Host Control Protocol (DHCP) server to perform DDNS updates of forward or A RRs in the primary DNS server, unless the DHCP server reports in the ACK FQDN option that it has overridden the client request and updated this information previously. The keywords are as follows:

- **both**—Enables the DHCP server to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously.

Note If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This instructs the server that it should attempt to dynamically update both the A and PTR RRs.

- **none**—On the client side, specifies that the DHCP client should include the FQDN option, however, it should not attempt any DDNS updates. On the server side, specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this and do the updates anyway.

Note If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Defaults

No default behavior.

Command Modes

Global 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

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp client update dns** command (no hyphen) is the interface configuration command.

If you specify the **both** and **none** keywords, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. The DHCP server can override the DHCP client using the **ip dhcp update dns override** command.

If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

If the FQDN option is included in the DHCP interaction, then the client may instruct the server to update "reverse" (the default), "both", or "none." Obviously, if the **ip ddns update method** command is configured with the **ddns both** keyword combination, then the FQDN option configuration should reflect an IP DHCP client update DNS server none, but you have to configure the system correctly.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

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

Examples

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

```
ip dhcp-client update dns server both
```

Related Commands

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

ip dhcp update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs) for most address pools, use the **ip dhcp update dns** command in global configuration mode. To disable dynamic updates, use the **no** form of this command.

ip dhcp update dns [**both**] [**override**] [**before**]

no ip dhcp update dns [**both**] [**override**] [**before**]

Syntax Description

both	(Optional) Enables the Dynamic Host Control Protocol (DHCP) server to perform DDNS updates on both A and PTR RRs unless the DHCP client has specified that the server not perform the updates in the fully qualified domain name (FQDN) option.
override	(Optional) Enables the DHCP server to override the DHCP client specification not to perform DDNS updates for both the A and PTR RRs.
before	(Optional) Enables the DHCP server to perform DDNS updates before sending the DHCP ACK back to the DHCP client.

Defaults

Perform DDNS updates after sending a DHCP ACK.

Command Modes

Global 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

Some address pools are configured using the **update dns** command, and that configuration overrides the global configuration. See the **update dns** command for more information.

If you specify the **both** and **override** keywords, the DHCP server will perform the updates for both A and PTR RRs overriding anything that the DHCP client has specified in the FQDN option.

Examples

The following example shows how to configure the DHCP server to perform A and PTR RR updates and to override the DHCP client FQDN option:

```
ip dhcp update dns both override
```

Related Commands

Command	Description
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

ip dns name-list

To add a hostname pattern-matching rule to the end of a Domain Name System (DNS) name list, use the **ip dns name-list** command in global configuration mode. To remove a rule from a DNS name list or to remove an entire name-list, use the **no** form of this command.

ip dns name-list *name-list-number* {**deny** | **permit**} *pattern*

no ip dns name-list *name-list-number* [{**deny** | **permit**} *pattern*]

Syntax Description

name-list-number	Integer from 1 to 500 that identifies the DNS name list.
deny	Specifies that any name matching the specified pattern immediately terminates matching the name list with a negative result.
permit	Specifies that any name matching the specified pattern immediately terminates matching the name list with a positive result.
pattern	Regular expression, case-insensitive, to be compared to the a DNS query hostname.

Command Default

No DNS name list is defined or modified. The access list defaults to an implicit **deny .*** clause. The access list is always terminated by an implicit **deny .*** clause.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command adds a hostname pattern-matching rule to the end of the specified DNS name list. A DNS name list is identified by a unique *name-list-number* value and defines an ordered list of hostname pattern-matching rules that the Cisco IOS software can use to match hostnames in a DNS query.

If the DNS name list does not exist yet, it is automatically created.

When a DNS name list is used to determine if a DNS view list member can be used to handle an incoming DNS query, the individual deny and permit clauses function as follows:

- If the query hostname matches the pattern in a deny clause, the DNS view is rejected; the view-selection process moves on to the next member of the DNS view list.
- If the query hostname matches the pattern in a permit clause, the DNS view is selected to handle the query; the view-selection process is finished.
- There is an implicit deny statement at the end of the access list. If the view-selection process reaches the end of the DNS name list without either a deny clause that causes the view to be rejected or a permit clause that causes the view to be selected, the DNS view is rejected; the view-selection process moves onto the next member of the DNS view list.

For any DNS name list number, the **ip dns name-list** command can be entered multiple times to specify any number of pattern-matching rules in a single name list.

To display a particular DNS name list or all configured name lists, use the **show ip dns name-list** command.

Use of Pattern Matching Characters to Specify the Hostname Pattern

Any rule in a DNS name list can include Cisco regular expression pattern-matching characters in the regular expression that defines the hostname pattern. For a detailed description of regular expressions and regular expression pattern-matching characters, see the *Cisco IOS Terminal Services Configuration Guide*.

Use of a DNS Name List Definition

A DNS name list can be referenced by a DNS view list (accessed by using the **ip dns view-list** command), within a DNS view list member definition (accessed by using the **view** command) that has been configured to deny or permit the use of that DNS view for handling a given DNS query based on whether the destination hostname adheres to a particular DNS name list. To configure this type of usage restriction on the view list member, use the **restrict name-group** command.

Examples

The following example shows how to configure DNS name list number 9 so that the name list will be matched if the query hostname matches either www.example2.com or *.example3.com:

```
Router(config)# ip dns name-list 9 permit www.example2.com
Router(config)# ip dns name-list 9 permit .*.example3.org
```

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns name-list	Displays a particular DNS name list or all configured name lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip dns primary

To configure the router as authoritative for a zone, use the **ip dns primary** command in global configuration mode. To configure the router as nonauthoritative for a zone, use the **no** form of this command.

ip dns primary *domain-name* **soa** *primary-server-name mailbox-name* [*refresh-interval* [*retry-interval* [*expire-ttl* [*minimum-ttl*]]]]

no ip dns primary *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS).
soa	Start of authority record parameters.
primary-server-name	Authoritative name server.
mailbox-name	DNS mailbox of administrative contact.
refresh-interval	(Optional) Refresh time in seconds. This time interval must elapse between each poll of the primary by the secondary name server. The range is from 0 to 4294967295. The default is 21600 (6 hours).
retry-interval	(Optional) Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed. The range is from 0 to 4294967295. The default is 900 (15 minutes).
expire-ttl	(Optional) Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval. The range is from 0 to 4294967295. The default is 7776000 (90 days).
minimum-ttl	(Optional) Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time. The range is from 0 to 4294967295. The default is 86400 (1 day).

Command Default

No authority record parameters are configured for the DNS name server, so queries to the DNS server for locally defined hosts will not receive authoritative responses from this server.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to configure the router as an authoritative name server for the host table, or zone file, of a DNS domain. The primary name server name and a DNS mailbox name are required authority record parameters. Optionally, you can override the default values for the polling refresh interval, the refresh retry interval, the authority expire time, and the minimum TTL for zone information.

To display the authoritative name server configuration for the router, use the **show ip dns primary** command.

Examples

The following example shows how to configure the router as the primary DNS server authoritative for the example.com domain, or zone:

```
Router(config)# ip dns primary example.com soa ns1.example.com mb1.example.com 10800 900
5184000 172800
```

In the above example, the DNS domain name of the router is ns1.example.com, and the administrative contact for this zone is mb1@example.com. The refresh time is 3 hours, the refresh retry time is 15 minutes, the authority expire time is 60 days, and the minimum TTL is 2 days.

Related Commands

Command	Description
ip dns server	Enables the DNS server on a router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show ip dns primary	Displays the authoritative name server configuration for the router.

ip dns server queue limit

To configure a limit to the size of the queues used by the Domain Name System (DNS) server processes, use the **ip dns server queue limit** command in global configuration mode. To remove any limit on the queue, use the **no** form of this command.

ip dns server queue limit forwarder *queue-size-limit*

no ip dns server queue limit forwarder

Syntax Description

forwarder	Sets the queue limit for the forwarder queue.
queue-size-limit	Specifies the maximum size to be used for the queue. Valid range is from 0 to 1000000. Value 0 indicates no limit.

Command Default

The queue limit is set to 0, indicating there is no limit on the queue.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(24)T	The **director** keyword was removed.

Usage Guidelines

When a DNS query is forwarded to another nameserver for resolution, some memory space is held for the corresponding DNS query until an appropriate response is received or until there is a timeout. If the queries are being received at a very high rate, this may result in the free I/O memory getting exhausted.

Use the **ip dns server queue limit** command to set a limit to the size of the queue.

Examples

The following example shows how to set the limit to the forwarder queue used by the DNS server:

```
Router(config)# ip dns server queue limit forwarder 10
Router(config)#
```

Related Commands

Command	Description
show ip dns statistics	Displays packet statistics for the DNS server.

ip dns server view-group

To specify the default Domain Name System (DNS) server view list for the router, use the **ip dns server view-group** command in global configuration mode. To remove this definition, use the **no** form of this command.

ip dns server view-group *view-list-name*

no ip dns server view-group

Syntax Description

view-list-name	Name of a DNS view list. **Note** If the specified view list does not exist, a warning is displayed but the default view list setting is configured anyway. The specified view list can be defined after the default DNS server view list is configured.

Command Default

No default DNS view list is configured; incoming queries arriving on an interface not assigned a specific DNS view list will be handled using the global default view.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command configures the router to use the specified DNS server view list as the default DNS view list. The default DNS view list is used to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list. The router checks these types of DNS queries against the DNS view list entries (in the order specified in the DNS view list) and uses the first DNS view list member whose restrictions allow the view to handle that query.

To specify that the router uses a particular DNS view list to choose the DNS view to use to handle incoming DNS queries that arrives on a specific interface, use the **ip dns view-group** command.

Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a “view list” when it is defined and as a “view group” when it is referenced in other commands.

Examples

The following example shows how to configure the DNS name list userlist1 as the default name list:

```
Router(config)# ip dns server view-group userlist1
```

Related Commands

Command	Description
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns spoofing

To enable Domain Name System (DNS) spoofing, use the **ip dns spoofing** command in global configuration mode. To disable DNS spoofing, use the **no** form of this command.

ip dns spoofing [*ip-address*]

no ip dns spoofing [*ip-address*]

Syntax Description

ip-address	(Optional) IP address used in replies to DNS queries.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

DNS spoofing allows a router to act as a proxy DNS server and “spoof” replies to any DNS queries using either the configured IP address in the **ip dns spoofing** command or the IP address of the incoming interface for the query. This functionality is useful for devices where the interface toward the ISP is not up. Once the interface to the ISP is up, the router forwards DNS queries to the real DNS servers.

The router will respond to the DNS query with the configured IP address when queried for any host name other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own host name.

The host name used in the DNS query is defined as the exact configured host name of the router specified by the **hostname** command, with no default domain appended. For example, in the following configuration:

```
ip domain name cisco.com
hostname host1
```

The system would respond with a DNS spoofing reply if queried for “host1” but not for “host1.cisco.com”.

Examples

In the following example, the router will respond to a DNS query with an IP address of 192.168.15.1:

```
ip dns spoofing 192.168.15.1
```

ip dns view

To access or create the Domain Name System (DNS) view of the specified name associated with the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance and then enter DNS view configuration mode so that forwarding and routing parameters can be configured for the view, use the **ip dns view** command in global configuration mode. To remove the definition of the specified DNS view and then return to global configuration mode, use the **no** form of this command.

ip dns view [**vrf** *vrf-name*] {**default** | *view-name*}

no ip dns view [**vrf** *vrf-name*] {**default** | *view-name*}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view. Default is to associate the DNS view with the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is created anyway. The specified VRF can be defined after the DNS view is configured. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	Refers to the unnamed DNS view.
view-name	String (not to exceed 64 characters) that specifies the name of the DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Default

No new DNS view is accessed or created.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enters DNS view configuration mode—for the specified DNS view—so that forwarding parameters, resolving parameters, and the logging setting can be configured for that view. If the specified DNS view does not exist yet, it is automatically created.

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

The default view associated with the unnamed global VRF exists by default. This is the view that is referenced by using the **ip dns view** command without specifying a VRF and specifying the **default** keyword instead of a *view-name* argument. The default DNS view cannot be removed.

Different DNS views can be associated with the same VRF.

To enable debugging output for DNS view events, use the **debug ip dns view** command.

To display information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used, use the **show ip dns view** command.

Subsequent Operations on a DNS View Definition

After you use the **ip dns view** command to define a DNS view and enter DNS view configuration mode, you can configure DNS forwarder parameters, DNS resolution parameters, and system message logging for the view.

To configure the Cisco IOS DNS forwarder functionality, use the following commands:

- **dns forwarder**
- **dns forwarding**
- **dns forwarding source interface**

To configure the Cisco IOS DNS resolver functionality, use the following commands:

- **domain list**
- **domain lookup**
- **domain multicast**
- **domain name**
- **domain name-server**
- **domain name-server interface**
- **domain retry**
- **domain round-robin**
- **domain timeout**

To enable logging of a system message logging (syslog) message each time the DNS view is used, use the **logging** command.

Use of a DNS View Definition

After a DNS view is configured, the view can be added to a DNS view list (by using the **ip dns view-list** command) and usage restrictions for that view within that view list can configured (by using the **restrict name-group** and **restrict source access-grou**p commands).

Examples

The following example shows how to define the default DNS view in the global address space. This DNS view exists by default, and it is the view that has been in use since before the Split DNS feature was implemented.

```
Router(config)# ip dns view default
```

The following example shows how to define the default DNS view associated with VRF vpn101, creating the view if it does not already exist:

```
Router(config)# ip dns view vrf vpn101 default
```

The following example shows how to define the DNS view user2 in the global address space, creating the view if it does not already exist:

```
Router(config)# ip dns view user2
```

The following example shows how to define the DNS view user2 associated with VRF vpn101, creating the view if it does not already exist:

```
ip dns view vrf vpn101 user2
```

Related Commands

Command	Description
debug ip dns view	Enables debugging output for DNS view events.
dns forwarder	Specifies the ordered list of IP addresses to use when forwarding incoming DNS queries handled using the DNS view.
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 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.
domain lookup	Enables the IP DNS-based hostname-to-address translation for internally generated DNS queries handled using the DNS view.
domain multicast	Specifies the IP address to use for multicast lookups handled using the DNS view.
domain name	Specifies a single default domain name to use to complete unqualified hostnames in internally generated 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.
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.
domain retry	Specifies the number of times to retry sending or forwarding a DNS query handled using the DNS view.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
domain timeout	Specifies the amount of time to wait for a response to a sent or forwarded DNS query handled using the DNS view.

Command	Description
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
logging	Enables logging of a syslog message each time the DNS view is used.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

ip dns view-group

To attach a Domain Name System (DNS) view list to the interface, use the **ip dns view-group** command in interface configuration mode. To disable the attachment of a DNS view list to an interface, use the **no** form of this command.

ip dns view-group *view-list-name*

no ip dns view-group *view-list-name*

Syntax Description

view-list-name	Name of an existing DNS view list. **Note** If the specified view list does not exist, a warning is displayed and the view list setting is not configured for the interface.

Command Default

No DNS view list is attached to the interface. If a default DNS view list is configured, that view list is used to handle incoming DNS queries. If no view list has been configured either on this specific interface or for the system, incoming DNS queries are handled using the default global view.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command configures the router to use the specified DNS view list to choose which DNS view to use to handle incoming DNS queries that arrive on the interface.

Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

A DNS view list can also be configured as the default DNS view list (by using the **ip dns server view-group** command) to determine which DNS view the router will use to handle a given incoming DNS query that arrives on an interface that is not configured with a DNS view list.

Note The *view-list-name* argument referenced in this command is configured using the **ip dns view-list** command. The DNS view list is referred to as a “view list” when it is defined and as a “view group” when it is referenced in other commands.

When an incoming DNS query is received through the interface, the Cisco IOS software will check the members of the DNS view list—in the order specified in the view list—to determine if the usage restrictions on any view list member allow the view to be used to forward the incoming query:

- Each DNS view list member is checked, in the order specified by the list.
- The first DNS view in the view list with configured usage restrictions (based on the query destination hostname or the query source IP address) that allow its use for the query will be used to forward the incoming query.

  If the hostname cache for the view contains the information needed to answer the query, the router will respond to the query with the hostname IP address in that internal cache. Otherwise, provided DNS forwarding is enabled for the DNS view, the router will forward the query to the configured name servers (each in turn, until a response is received), and the response will be both added to the hostname cache and sent back to the originator of the query.
- If no DNS view in the DNS view list is qualified to handle the query, the router drops the query.

Examples

The following example shows how to configure the router so that each time a DNS query arrives through interface ethernet0 the usage restrictions for the members of the DNS view list userlist2 are checked in the order specified by the view list definition. The router uses the first view list member whose usage restrictions allow that DNS view to forward the query.

```
Router(config)# interface ethernet0
Router(config-if)# ip dns view-group userlist2
```

Related Commands

Command	Description
interface	Selects an interface to configure.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

ip dns view-list

To access or create the Domain Name System (DNS) view list of the specified name and then enter DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS view members, use the **ip dns view-list** command in global configuration mode. To remove the definition of the specified DNS view list, use the **no** form of this command.

ip dns view-list *view-list-name*

no dns view-list *view-list-name*

Syntax Description

view-list-name	Text string (not to exceed 64 characters) that uniquely identifies the DNS view list to be created.

Command Default

No DNS view list is accessed or created.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enters DNS view list configuration mode—for the specified view list—so that individual view list members (DNS views and their order numbers within the view list) can be accessed in, added to, or deleted from that view list. If the specified DNS view list does not exist yet, it is automatically created.

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

To display information about a specific DNS view list or all currently configured DNS view lists, use the **show ip dns view-list** command.

Subsequent Operations on a DNS View List

After you use the **ip dns view-list** command to define a DNS view list and enter DNS view list configuration mode, you can use the **view** command to access a view list member or add a DNS view as a new view list member at the end of the list. Each view list member specifies a DNS view and a value that indicates the relative order for checking that view when the DNS view list is used. to determine if it can be used to address a DNS query.

For any DNS view list member, you can use the **restrict authenticated**, **restrict name-group**, and **restrict source access-group** commands to configure usage restrictions for the DNS view list member. These restrictions are based on query source authentication, the query hostname, and the query source host IP address, respectively.

Purpose of a DNS View List

When a DNS view list is used to select a DNS view to use to handle a given DNS query, the Cisco IOS software checks each DNS view in the DNS view list—in the order specified in the view list—to determine if the usage restrictions for that view allow the view to be used to address that particular DNS query.

The first DNS view with configured usage restrictions that allow its use for the DNS query will be used to resolve or forward the query. That is, the router will use the configuration parameters for that DNS view to either respond to the query (by using the name cache belonging to the DNS view) or forward the query to the configured name servers. If no DNS view in the view list is qualified to handle the query, the router does not send or forward the query.

Note Multiple DNS view list definitions enable you to use the same DNS view, but with different restrictions, depending on the source of the DNS query being processed. For example, in one DNS view list a particular DNS view could be used with very few usage restrictions, while in another DNS view list the same DNS view could be used with more usage restrictions.

Use of a DNS View List for DNS Queries Incoming from a Particular Interface

Use the **ip dns view-group** command to configure the router to use a particular DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on that interface. Only one DNS view list can be assigned to a given interface. However, a single DNS view list can be assigned to any number of interfaces so that the same ordered list of DNS views (along with the restrictions specified in the view list) can be checked by multiple interfaces.

Use of a DNS View List as the Default DNS View List

Use the **ip dns server view-list** command to configure the default DNS view list. The router uses the default DNS view list to determine which DNS view to use to handle incoming DNS queries that arrive on an interface that is not configured with a DNS view list.

Examples

The following example shows how to remove the DNS view user1 from the DNS view list userlist5 and then add the view back to the view list, but with a different position indicator specified for that member within the view list. A usage restriction is also added to the view list member user1.

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# no view user1 30
Router(cfg-dns-view-list)# view user1 10
Router(cfg-dns-view-list)# restrict name-group 7
```

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming queries that arrive on an interface not configured with a DNS view list.

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
restrict authenticated	Restricts the use of the DNS view list member to DNS queries for which the DNS query host can be authenticated.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.
view	Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.

ip domain list

To define a list of default domain names to complete unqualified names, use the **ip domain list** command in global configuration mode. To delete a name from a list, use the **no** form of this command.

ip domain list [**vrf** *vrf-name*] *name*

no ip domain list [**vrf** *vrf-name*] *name*

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Defaults

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-list** to **ip domain list**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list** command you can define a list of domains, each to be tried in turn until the system finds a match.

If the **ip domain list vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, **ip domain-list**.

Examples

The following example shows how to add several domain names to a list:

```
ip domain list company.com
ip domain list school.edu
```

The following example shows how to add several domain names to a list in vpn1 and vpn2:

```
ip domain list vrf vpn1 company.com
ip domain list vrf vpn2 school.edu
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain lookup

To enable the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable the DNS, use the **no** form of this command.

ip domain lookup [**source-interface** *interface-type interface-number* | **nsap**]

no ip domain lookup [**source-interface** *interface-type interface-number* | **nsap**]

Syntax Description

source-interface	(Optional) Specifies the source interface for DNS resolver.
interface-type interface-number	(Optional) The interface type and number.
nsap	(Optional) Enables IP DNS queries for Connectionless Network Service (CLNS) and Network Service Access Point (NSAP) addresses.

Command Default

The IP DNS-based host name-to-address translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2	This command was modified. The syntax of the command changed from **ip domain-lookup** to **ip domain lookup**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. The **nsap** keyword was added.

Usage Guidelines

The Cisco IOS software will still accept the previous version of the command, which is **ip domain-lookup**. If the **ip domain lookup** command is enabled on a router, and you execute the **show tcp brief** command, the response time of the router to display the output is very slow. With both IP and ISO CLNS enabled on a router, the **ip domain lookup nsap** command allows you to discover a CLNS address without having to specify a full CLNS address given a host name. This command is useful for the **ISO CLNS ping EXEC** command and when making CLNS Telnet connections.

Examples

The following example enables the IP DNS-based host name-to-address translation:

```
Router# configure terminal
Router(config)# ip domain lookup
Router(config)# end
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
show tcp brief	Displays a concise description of TCP connection endpoints.

ip domain name

To define a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **ip domain name** command in global configuration mode. To disable use of the Domain Name System (DNS), use the **no** form of this command.

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

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

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-name** to **ip domain name**.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and cisco.com appended to it before being added to the host table.

If the **ip domain name vrf** command option is specified, the domain names are only used for name queries in the specified VRF.

The Cisco IOS software will still accept the previous version of the command, which is **ip domain-name**.

Examples

The following example shows how to define cisco.com as the default domain name:

```
ip domain name cisco.com
```

The following example shows how to define cisco.com as the default domain name for vpn1:

```
ip domain name vrf vpn1 cisco.com
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain retry

To specify the number of times to retry sending Domain Name System (DNS) queries, use the **ip domain retry** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip domain retry *number*

no ip domain retry *number*

Syntax Description

number	Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 100; the default is 2.

Defaults

number: 2 times

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the **ip domain retry** command is not configured, the Cisco IOS software will only send DNS queries out twice.

Examples

The following example shows how to configure the router to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain round-robin

To enable round-robin functionality on DNS servers, use the **ip domain round-robin** command in global configuration mode. To disable round-robin functionality, use the no form of the command.

ip domain round-robin

no ip domain round-robin

Syntax Description

This command has no arguments or keywords.

Defaults

Round robin is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)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

In a multiple server configuration *without* the DNS round-robin functionality, the first host server/IP address is used for the whole time to live (TTL) of the cache, and uses the second and third only in the event of host failure. This behavior presents a problem when a high volume of users all arrive at the first host during the TTL time. The network access server (NAS) then sends out a DNS query; the DNS servers reply with a list of the configured IP addresses to the NAS. The NAS then caches these IP addresses for a given time (for example, five minutes). All users that dial in during the five minute TTL time will land on one host, the first IP address in the list.

In a multiple server configuration *with* the DNS round-robin functionality, the DNS server returns the IP address of all hosts to rotate between the cache of host names. During the TTL of the cache, users are distributed among the hosts. This functionality distributes calls across the configured hosts and reduces the amount of DNS queries.

Examples

The following example allows a Telnet to www.company.com to connect to each of the three IP addresses specified in the following order: the first time the Telnet command is given, it would connect to 10.0.0.1; the second time the command is given, it would connect to 10.1.0.1; and the third time the command is given, it would connect to 10.2.0.1. In each case, the other two addresses would also be tried if the first one failed; this is the normal operation of the Telnet command.

```
ip host www.server1.com 10.0.0.1 10.1.0.1 10.2.0.1
ip domain round-robin
```

ip domain timeout

To specify the amount of time to wait for a response to a DNS query, use the **ip domain timeout** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip domain timeout *seconds*

no ip domain timeout *seconds*

Syntax Description

seconds	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600; the default is 3.

Defaults

seconds: 3 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the **ip domain timeout** command is not configured, the Cisco IOS software will only wait 3 seconds for a response to a DNS query.

Examples

The following example shows how to configure the router to wait 50 seonds for a response to a DNS query:

```
ip domain timeout 50
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain retry	Specifies the number of times to retry sending DNS queries.
ip domain timeout	Specifies the amount of time to wait for a response to a DNS query.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip 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) and to enter host-list configuration mode, use the **ip host-list** command in global configuration mode. To disable the host list, use the **no** form of this command.

ip host-list *host-list-name* [**vrf** *vrf-name*]

no ip host-list *host-list-name* [**vrf** *vrf-name*]

Syntax Description

host-list-name	List of servers that will receive DDNS updates.
vrf *vrf-name*	(Optional) Identifies the virtual routing and forwarding (VRF) table. The *vrf-name* argument identifies the address pool to which the VRF is associated.

Defaults

No IP host list is configured.

Command Modes

Global 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

The interface configuration overrides the global configuration.

Examples

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

```
ip host-list test
 host vrf testgroup
```

Related Commands

Command	Description
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RR.

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

no ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

Syntax Description

vrf *vrf-name*	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The *vrf-name* argument specifies a name for the VRF table.
server-address1	IPv4 or IPv6 addresses of a name server.
server-address2...server-address6	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Command Default

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	Support for IPv6 addresses was added.
12.0(21)ST	Support for IPv6 addresses was added.
12.0(22)S	Support for IPv6 addresses was added.
12.2(14)S	Support for IPv6 addresses was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
ip name-server 172.16.1.2
```

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers for vpn1:

```
Router(config)# ip name-server vrf vpn1 172.16.1.111 172.16.1.2
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted decimal domain name).

logging (DNS)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging

no logging

Syntax Description

This command has no arguments or keywords.

Command Default

No syslog message is logged when the DNS view is used.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables the logging of syslog messages for the DNS view.

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

Examples

The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

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

Related Commands

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the 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.

restrict authenticated

To specify that a Domain Name System (DNS) view list member cannot be used to respond to an incoming DNS query if the DNS view and the DNS client have not been authenticated, use the **restrict authenticated** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict authenticated

no restrict authenticated

Syntax Description

This command has no arguments or keywords.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the DNS view and the DNS client have been authenticated.

Command Modes

DNS view list member configuration

Command History

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

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query unless the Cisco IOS software has verified the authentication status of the client. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if the client is not authenticated. The router that is running Split DNS determines the query client authentication status by calling any DNS client authentication functions that have been registered with Split DNS.

A client can be authenticated within a Cisco IOS environment by various methods, such as Firewall Authentication Proxy, 802.1x, and wireless authentication. Some DNS authentication functions might inspect only the source IP address or MAC address and the VRF information, while other functions might inspect the source IP address or MAC address, the VRF information, and the DNS view name.

Note In Cisco IOS Release 12.4(9)T, none of these authentication methods are implemented by any Cisco IOS authentication subsystems. As a result, if a DNS view is configured to be restricted based on client authentication, the Cisco IOS software will not use that view whenever the view is considered for handling a query. In future Cisco IOS releases, authentication subsystems will implement client authentication functions and enable them to be registered on a router running Split DNS. This will enable the Cisco IOS software to support authentication-based use restrictions on DNS views. This command is provided now for backward compatibility when DNS authentication functions are implemented.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the query source IP address (configured by using the **restrict source access-group** command) or the query hostname (configured by using the **restrict name-group** command).

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Examples

The following example shows how to create the DNS view list userlist5 so that it contains the two DNS views:

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view vrf vpn101 user1 20
Router(cfg-dns-view-list-member)# exit
Router(cfg-dns-view-list)# view vrf vpn201 user2 35
Router(cfg-dns-view-list-member)# restrict authenticated
```

Both view list members are restricted from responding to an incoming DNS query unless the query is from the same VRF as the VRF with which the view is associated.

The first view list member (the view named user1 and associated with the VRF vpn101) has no further restrictions placed on its use.

The second view list member (the view named user2 and associated with the VRF vpn201) is further restricted from responding to an incoming DNS query unless the Cisco IOS software can verify the authentication status of the client.

Related Commands

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

restrict name-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the query hostname matches a permit clause in a particular DNS name list and none of the deny clauses, use the **restrict name-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict name-group *name-list-number*

no restrict name-group *name-list-number*

Syntax Description

name-list-number	Integer from 1 to 500 that identifies an existing DNS name list.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the query hostname matches a permit clause in a particular DNS name list.

Command Modes

DNS view list member configuration

Command History

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

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if a permit clause in the specified DNS name list specifies a regular expression that matches the query hostname. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if an explicit deny clause in the name list (or the implicit deny clause at the end of the name list) matches the query hostname. To configure a DNS name list, use the **ip dns name-list** command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the source IP address of the incoming DNS query. To configure this type of restriction, use the **restrict source access-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *name-list-number* argument referenced in this command is configured using the **ip dns name-list** command. The DNS name list is referred to as a “name list” when it is defined and as a “name group” when it is referenced in other commands.

Examples

The following example shows how to specify that DNS view user3 associated with the global VRF, when used as a member of the DNS view list userlist5, cannot be used to respond to an incoming DNS query unless the query hostname matches the DNS name list identified by the number 1:

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# restrict name-group 1
```

Related Commands

Command	Description
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

restrict source access-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the source IP address of the DNS query matches a standard access control list (ACL), use the **restrict source access-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict source access-group {*acl-name* | *acl-number*}

no restrict source access-group {*acl-name* | *acl-number*}

Syntax Description

acl-name	String (not to exceed 64 characters) that specifies a standard ACL.
acl-number	Integer from 1 to 99 that specifies a standard ACL.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the source IP address of the DNS query belongs to a particular standard ACL.

Command Modes

DNS view list member configuration

Command History

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

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if the query source IP address matches the specified standard ACL. To configure a standard ACL, use the **access-list** (IP standard) command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the the query hostname. To configure this type of restriction, use the **restrict name-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source Virtual Private Network (VPN) routing and forwarding (VRF) instance of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *acl-name* or *acl-number* argument referenced in this command is configured using the **access-list** command. The access list is referred to as a "access list" when it is defined and as a "access group" when it is referenced in other commands.

Examples

The following example shows how to specify that DNS view user4 associated with the global VRF, when used as a member of the DNS view list userlist7, cannot be used to respond to an incoming DNS query unless the query source IP address matches the standard ACL number 6:

```
Router(config)# ip dns view-list userlist7
Router(cfg-dns-view-list)# view user4 40
Router(cfg-dns-view-list-member)# restrict source access-group 6
```

Related Commands

Command	Description
access-list (IP standard)	Creates a standard ACL that defines the specific host or subnet for host-specific PAM.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

show ip ddns update

To display information about the Dynamic Domain Name System (DDNS) updates, use the **show ip ddns update** command in privileged EXEC mode.

show ip ddns update [*interface-type number*]

Syntax Description

interface-type number	(Optional) Displays DDNS updates configured on an interface.

Command Modes

Privileged EXEC

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 output shows the IP DDNS update method on loopback interface 100 and the destination:

```
Router# show ip ddns update

Dynamic DNS Update on Loopback100:
 Update Method Name     Update Destination
 testing                10.1.2.3
```

Related Commands

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

show ip ddns update method

To display information about the Dynamic Domain Name System (DDNS) update method, use the **show ip ddns update method** command in privileged EXEC mode.

show ip ddns update method [*method-name*]

Syntax Description

method-name	(Optional) Name of the update method.

Command Modes

Privileged EXEC

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 is sample output from the **show ip ddns update method** command:

```
Router# show ip ddns update method

Dynamic DNS Update Method: test
  Dynamic DNS update in IOS internal name cache
```

Related Commands

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

show ip dns name-list

To display a particular Domain Name System (DNS) name list or all configured DNS name lists, use the **show ip dns name-list** command in privileged EXEC mode.

show ip dns name-list [*name-list-number*]

Syntax Description

name-list-number	(Optional) Integer from 1 to 500 that identifies a DNS name list.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Display a DNS name list to view the ordered list of pattern-matching rules it defines. Each rule in the name list specifies a regular expression and the type of action to be taken if the query hostname matches that expression.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Examples

The following is sample output from the **show ip dns name-list** command:

```
Router# show ip dns name-list

ip dns name-list 1
   deny WWW.EXAMPLE1.COM
   permit WWW.EXAMPLE.com

ip dns name-list 2
   deny WWW.EXAMPLE2.COM
   permit WWW.EXAMPLE3.COM
```

Table 18 describes the significant fields shown for each DNS name list in the display.

Table 18 show ip dns name-list Field Descriptions

Field	Description
name-list	Integer that identifies the DNS name list. Configured using the **ip dns name-list** command.
deny	Regular expression, case-insensitive, to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name list will be determined to have not matched the hostname. A deny clause is configured by using the **ip dns name-list** command.
permit	Regular expression in domain name format (a sequence of case-insensitive ASCII labels separated by dots), case-insensitive, and to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name-list will be determined to have matched the hostname. A permit clause is configured by using the **ip dns name-list** command.

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.

show ip dns primary

To display the authority record parameters configured for the Domain Name System (DNS) server, use the **show ip dns primary** command in user EXEC or privileged EXEC mode.

show ip dns primary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example shows how to configure the router as a DNS server and then display the authority record parameters for the DNS server:

```
Router(conf)# ip dns server
Router(conf)# ip dns primary example.com soa ns1.example.com mb1.example.com
Router(conf)# ip host example.com ns ns1.example.com
Router(conf)# ip host ns1.example.com 209.165.201.1
Router(conf)# exit
Router# show ip dns primary
Primary for zone example.com:
  SOA information:
  Zone primary (MNAME): ns1.example.com
  Zone contact (RNAME): mb1.example.com
  Refresh (seconds):    21600
  Retry (seconds):      900
  Expire (seconds):     7776000
  Minimum (seconds):    86400
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip dns primary Field Descriptions

Field	Description
Zone primary (MNAME)	Authoritative name server.
Zone contact (RNAME)	DNS mailbox of administrative contact.
Refresh (seconds)	Refresh time in seconds. This time interval that must elapse between each poll of the primary by the secondary name server.
Retry (seconds)	Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed.

Table 19 show ip dns primary Field Descriptions (continued)

Field	Description
Expire (seconds)	Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval.
Minimum (seconds)	Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time.

Related Commands

Command	Description
ip dns primary	Configures router authority parameters for the DNS name server,for the DNS name server.
ip dns server	Enables the DNS server on the router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

show ip dns statistics

To display packet statistics for the Domain Name System (DNS) server, use the **show ip dns statistics** command in user EXEC or privileged EXEC mode.

show ip dns statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use this command to display the number of DNS requests received and dropped by the DNS server and the number of DNS responses sent by the DNS server.

Examples

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

```
Router# show ip dns statistics

DNS requests received = 818725 ( 818725 + 0 )
DNS requests dropped = 0 ( 0 + 0 )
DNS responses replied = 0 ( 0 + 0 )

Forwarder queue statistics:
Current size = 0
Maximum size = 400
Drops = 804613

Director queue statistics:
Current size = 0
Maximum size = 0
Drops = 0
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip dns statistics Field Descriptions

Field	Description
DNS requests received	Total number of DNS requests received by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets received • Number of TCP packets received
DNS requests dropped	Total number of DNS requests discarded by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets dropped • Number of TCP packets dropped
DNS responses replied	Total number of DNS responses sent by the DNS server. Additional details are displayed in parenthesis: • Number of UDP packets dropped • Number of TCP packets dropped
Current size	Displays the current size of the queue counter.
Maximum size	Displays the maximum size of the queue counter reached since the reload. **Note** Whenever you change the queue size, the Maximum size counter will be reset to zero.
Drops	Displays the number of packets dropped when a queue function fails. **Note** Whenever you change the queue size, the Drops counter will be reset to zero.

show ip dns view

To display configuration information about a Domain Name System (DNS) view or about all configured DNS views, including the number of times the DNS view was used, the DNS resolver settings, the DNS forwarder settings, and whether logging is enabled, use the **show ip dns view** command in privileged EXEC mode.

show ip dns view [**vrf** *vrf-name*] [**default** | *view-name*]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Specifies that the DNS view is unnamed. By default all configured DNS views are displayed.
view-name	(Optional) Name of the DNS view whose information is to be displayed. Default is all configured DNS views. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Display DNS view information to view its DNS resolver settings, DNS forwarder settings, and whether logging is enabled.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Because different DNS views can be associated with the same VRF, omitting both the **default** keyword and the *view-name* argument causes this command to display information about all the views associated with the global or named VRF.

Examples

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

```
Router# show ip dns view

DNS View default parameters:
Logging is on (view used 102 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example.com
  Domain search list: example1.com example2.com example3.com
  Domain name for multicast lookups: 192.0.2.10
  Lookup timeout: 7 seconds
  Lookup retries: 5
  Domain name-servers:
    192.168.2.204
    192.168.2.205
    192.168.2.206
  Round-robin'ing of IP addresses is enabled
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.11
    192.168.2.12
    192.168.2.13
  Forwarder source interface: FastEthernet0/1

DNS View user5 parameters:
Logging is on (view used 10 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example5.net
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.104
    192.168.2.105
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.204

DNS View user1 vrf vpn101 parameters:
Logging is on (view used 7 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example1.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.100
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.200 (vrf vpn201)
```

Table 21 describes the significant fields shown for each DNS view in the display.

Table 21 show ip dns view Field Descriptions

Field	Description
Logging	Logging of a system message logging (syslog) message each time the DNS view is used. Configured using the **logging** command. **Note** If logging is enabled for a DNS view, the **show ip dns view** command output includes the number of times the DNS view has been used in responding to DNS queries.
Domain lookup	DNS lookup to resolve hostnames for internally generated queries. Enabled or disabled using the **domain lookup** command.
Default domain name	Default domain to append to hostnames without a dot. Configured using the **domain name** command.
Domain search list	List of domain names to try for hostnames without a dot. Configured using the **domain list** command.
Domain name for multicast lookups	IP address to use for multicast address lookups. Configured using the **domain multicast** command.
Lookup timeout	Time (in seconds) to wait for DNS response after sending or forwarding a query. Configured using the **domain timeout** command.
Lookup retries	Number of retries when sending or forwarding a query. Configured using the **domain retry** command.
Domain name-servers	Up to six name servers to use to resolve domain names for internally generated queries. Configured using the **domain name-server** command.
Resolver source interface	Source interface to use to resolve domain names for internally generated queries. Configured using the **ip domain lookup source-interfac**e global command.
Round robin'ing of IP addresses	Round-robin rotation of the IP addresses associated with the hostname in cache each time hostnames are looked up. Enabled or disabled using the **domain round-robin** command.
Forwarding of queries	Forwarding of incoming DNS queries. Enabled or disabled using the **dns forwarding** command.
Forwarder addresses	Up to six IP address to use to forward incoming DNS queries. Configured using the **dns forwarder** command.
Forwarder source-interface	Source interface to use to forward incoming DNS queries. Configured using the **dns forwarding source-interface** command.

show ip dns view-list

To display information about a Domain Name System (DNS) view list or about all configured DNS view lists, use the **show ip dns view-list** command in privileged EXEC mode.

show ip dns view-list [*view-list-name*]

Syntax Description

view-list-name	(Optional) Name of the DNS view list. Default is all configured DNS view lists.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

IP DNS view lists are defined by using the **ip dns view-list** command.

To display information about how DNS view lists are applied, use the **show running-config** command:

- The default DNS view list, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **ip dns server view-group** command).
- Any DNS view lists attached to interfaces are listed in the information for each individual interface (in the **interface** command information for that interface, as the argument for the **ip dns view-group** command).

Examples

The following is sample output from the **show ip dns view-list** command:

```
Router# show ip dns view-list

View-list userlist1:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
View-list userlist2:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to ip dns name-list: 151
```

Table 22 describes the significant fields shown for each DNS view list in the display.

Table 22 show ip dns view-list Field Descriptions

Field	Description
View-list	A DNS view list name. Configured using the **ip dns view** command.
View	A DNS view that is a member of this DNS view list. If the view is associated with a VRF, the VRF name is also displayed. Configured using the **ip dns view-list** command.
Evaluation order	Indication of the order in which the DNS view is checked, relative to other DNS views in the same DNS view list. Configured using the **view** command.
Restrict	Usage restrictions for the DNS view when it is a member of this DNS view list. Configured using the **restrict name-group** command or the **restrict source access-group** command.

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
interface	Configures an interface type and enter interface configuration mode so that the specific interface can be configured.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show running-config	Displays the contents of the currently running configuration file of your routing device.

show ip host-list

To display the assigned hosts in a list, use the **show ip host-list** command in privileged EXEC mode.

show ip host-list [*host-list-name*]

Syntax Description

host-list-name	(Optional) Name assigned to the list of hosts.

Command Modes

Privileged EXEC

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 is sample output from the **show ip host-list** command example for the abctest group:

```
Router# show ip host-list abctest

Host list: abctest
 ddns.abc.test
 10.2.3.4
 ddns2.unit.test
 10.3.4.5
 ddns3.com
 10.3.3.3
 e.org
 1.org.2.org
 3.com
 10.5.5.5 (VRF: def)
```

Related Commands

Command	Description
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.
host (host-list)	Specifies a list of hosts that will receive 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	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.

Command	Description
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.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

update dns

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

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

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

Syntax Description

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

Defaults

No updates are performed.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
update dns never
```

Related Commands

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

view (DNS)

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

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

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

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** If the named VRF does not exist, a warning is displayed but the view is added to the view list anyway. The specified VRF can be defined after the view is added as a member of the view list (and after the view itself is defined). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
default	Specifies that the DNS view is unnamed. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
view-name	String (not to exceed 64 characters) that identifies the name of an existing DNS view. **Note** If the specified view does not exist, a warning is displayed but the default view list member is added anyway. The specified view can be defined after it is added as a member of DNS view list. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name (or the **default** keyword) and the VRF with which it is associated.
order-number	Integer from 1 to 2147483647 that specifies the order in which the DNS view is checked, with respect to other DNS views in the same DNS view list. **Tip** If the *order-number* values for the DNS views within a DNS view list are configured with large intervals between them (for example, by specifying *order-number* values such as 10, 20, and 30), additional DNS views can be inserted into the view list quickly without affecting the existing ordering or views in the view list. That is, adding a new view to the view list—or changing the ordering of existing views within the view list—does not require that existing views in the view list be removed from the view list and then added back to the list with new *order-number* values.

Command Default

No DNS view is accessed or created.

Command Modes

DNS view list configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Subsequent Operations on a DNS View List Member

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

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

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

Reordering of DNS View List Members

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

Examples

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

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# exit
Router(cfg-dns-view-list)# no view vrf vpn102 user2 20
```

Related Commands

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

IP Addressing Commands

clear host

To delete hostname-to-address mapping entries from one or more hostname caches, use the **clear host** command in privileged EXEC mode.

clear host [**view** *view-name* | **vrf** *vrf-name* | **all**] {*hostname* | *****}

Syntax Description

view *view-name*	(Optional) The *view-name* argument specifies the name of the Domain Name System (DNS) view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.
all	(Optional) Specifies that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view.
hostname	Name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache.
*****	Specifies that all the hostname-to-address mappings are to be deleted from the specified hostname cache.

Command Default

No hostname-to-address mapping entries are deleted from any hostname cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	The **vrf** keyword, *vrf-name* argument, and **all** keyword were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command clears the specified hostname cache entries in running memory, but it does not remove the entries from NVRAM.

Entries can be removed from the hostname caches for a DNS view name, from the hostname caches for a VRF, or from all configured hostname caches. To remove entries from hostname caches for a particular DNS view name, use the **view** keyword and *view-name* argument. To remove entries from the hostname caches for a particular VRF, use the **vrf** keyword and *vrf-name* argument. To remove entries from all configured hostname caches, use the **all** keyword.

To remove entries that provide mapping information for a single hostname, use the *hostname* argument. To remove all entries, use the ***** keyword.

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 DNS hostname cache for a DNS view, use the **ip host** command.

Examples

The following example shows how to clear all entries from the hostname cache for the default view in the global address space:

```
Router# clear host all *
```

The following example shows how to clear entries for the hostname www.example.com from the hostname cache for the default view associated with the VPN named vpn101:

```
Router# clear host vrf vpn101 www.example.com
```

The following example shows how to clear all entries from the hostname cache for the view named user2 in the global address space:

```
Router# clear host view user2 *
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a 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.

clear ip route

To delete routes from the IP routing table, use the **clear ip route** command in EXEC mode.

clear ip route {*network* [*mask*] | *****}

Syntax Description

network	Network or subnet address to remove.
mask	(Optional) Subnet address to remove.
*****	Removes all routing table entries.

Defaults

All entries are removed.

Command Modes

EXEC

Command History

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

Examples

The following example removes a route to network 10.5.0.0 from the IP routing table:

```
Router> clear ip route 10.5.0.0
```

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 **no** form 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.
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.

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 classless

To enable a router to forward packets, which are destined for a subnet of a network that has no network default route, to the best supernet route possible, use the **ip classless** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip classless

no ip classless

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The default behavior changed from disabled to enabled.
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 allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table, and there is no network default route.

Note If the supernet or default route is learned by using Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), the **no ip classless** configuration command is ignored.

Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** command in global configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the router.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an Internet Control Message Protocol (ICMP) redirect message back. The ICMP redirect message indicates which local router the Cisco IOS software should use.

Examples

The following example defines the router on IP address 192.31.7.18 as the default router:

```
ip default-gateway 192.31.7.18
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t**_modem-telephone-number_} [*tcp-port-number*] {*ip-address1* [*ip-address2...ip-address8*] | **additional** *ip-address9* [*ip-address10...ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}

no ip host [**vrf** *vrf-name*] [**view** *view-name*] {*hostname* | **t**_modem-telephone-number_} [*tcp-port-number*] {*ip-address1* [*ip-address2...ip-address8*] **additional** *ip-address9* [*ip-address10...ip-addressn*] | [**mx** *preference mx-server-hostname* | **ns** *nameserver-hostname* | **srv** *priority weight port target*]}

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the name of the DNS view whose hostname cache is to store the mappings. Default is the default DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
hostname	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
t_modem-telephone-number_	Modem telephone number that is mapped to the IP host address for use in Cisco modem user interface mode. You must enter the letter "t" before the telephone number. **Note** This argument is not relevant to the Split DNS feature.
tcp-port-number	(Optional) TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
ip-address1	Associated host IP address.
ip-address2...ip-address8	(Optional) Up to seven additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

additional *ip-address9*	The *ip-address9* argument specifies an additional IP address to add to the hostname cache. **Note** The use of the optional additional keyword enables the addition of more than eight IP addresses to the hostname cache.
ip-address10...ip-addressn	Additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
mx *preference mx-server-hostname*	Mail Exchange (MX) resource record settings for the host: • *preference*—The order in which mailers select MX records when they attempt mail delivery to the host. The lower this value, the higher the host is in priority. Range is from 0 to 65535. • *mx-server-hostname*—The DNS name of the SMTP server where the mail for a domain name should be delivered. An MX record specifies how you want e-mail to be accepted for the domain specified in the *hostname* argument. **Note** You can have several MX records for a single domain name, and they can be ranked in order of preference.
ns *nameserver-hostname*	Name Server (NS) resource record setting for the host: • *nameserver-hostname*—The DNS name of the machine that provides domain service for the particular domain. Machines that provide name service do not have to reside in the named domain. An NS record lists the name of the machine that provides domain service for the domain indicated by the *hostname* argument. **Note** For each domain you must have at least one NS record. NS records for a domain must exist in both the zone that delegates the domain and in the domain itself.
srv *priority weight port target*	Server (SRV) resource record settings for the host: • *priority*—The priority to give the record among the owner SRV records. Range is from 0 to 65535. • *weight*—The load to give the record at the same priority level. Range is from 0 to 65535. • *port*—The port on which to run the service. Range is from 0 to 65535. • *target*—Domain name of host running on the specified port. The use of SRV records enables administrators to use several servers for a single domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a specific domain and receive the names of any available servers.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache for a DNS view.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The **mx** keyword and the *preference* and *mx-server-hostname* arguments were added.
12.0(7)T	The **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments were added.
12.2(1)T	The **ns** keyword and the *nameserver-hostname* argument were added.
12.4(4)T	The capability to map a modem telephone number to an IP host was added for the Cisco modem user interface feature.
12.4(4)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command adds the specified hostname-to-IP address mappings as follows:

- If no VRF name and no DNS view name is specified, the mappings are added to the global hostname cache.
- Otherwise, the mappings are added to the DNS hostname cache for a specific DNS view:
  - If only a DNS view name is specified, the specified mappings are created in the view-specific hostname cache.
  - If only a VRF name is specified, the specified mappings are created in the VRF-specific hostname cache for the default view.
  - If both a VRF name and a DNS view name are specified, the specified mappings are created in the VRF-specific hostname cache for the specified view.

If the specified VRF does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the specified view does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the hostname cache does not exist yet, it is automatically created.

To specify the machine that provides domain service for the domain, use the **ns** keyword and the *nameserver-hostname* argument

To specify where the mail for the host is to be sent, use the **mx** keyword and the *preference* and *mx-server-hostname* arguments.

To specify a host that offers a service in the domain, use thhe **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments.

To display the display 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, use the **show hosts** command.

Note If a global or VRF-specific DNS hostname cache contains hostnames that are associated with multiple IP addresses, round-robin rotation of the returned addresses can be enabled on a DNS view-specific basis (by using the **domain round-robin** command).

Examples

The following example shows how to add three mapping entries to the global hostname cache and then remove one of those entries from the global hostname cache:

```
Router(config)# ip host www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host www.example2.com 192.0.2.242
Router(config)# no ip host www.example1.com 192.0.2.141
```

The following example shows how to add three mapping entries to the hostname cache for the DNS view user3 that is associated with the VRF vpn101 and then remove one of those entries from that hostname cache:

```
Router(config)# ip host vrf vpn101 view user3 www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host vrf vpn101 view user3 www.example2.com 192.0.2.242
Router(config)# no ip host vrf vpn101 view user3 www.example1.com 192.0.2.141
```

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query 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.

ip hostname strict

To ensure that Internet hostnames comply with Section 2.1 of RFC 1123, use the **ip hostname strict** command in global configuration mode. To remove the restriction on hostnames, use the **no** form of this command.

ip hostname strict

no ip hostname strict

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, that is, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2SR	This command was introduced.

Usage Guidelines

Section 2.1 of RFC 1123 specifies the following rules for hostnames:

- A hostname is composed of one or more labels, separated by periods.
- Each label is composed of one or more of the following characters: letters (A-Z, a-z), digits (0-9), and the hyphen (-). No other characters are allowed.
- Alphabetic characters in hostnames can be either uppercase or lowercase, in any combination.
- A hyphen cannot be the first character of any label.
- The most significant label (also described as the top-level domain or TLD), that is, the group of characters that follow the final dot of the domain name, must contain at least one letter or hyphen, and must have least two characters.
- A hostname, including the periods, cannot have more than 255 characters. However, hostnames should not exceed 63 characters because conforming applications might be unable to handle hostnames longer than that.

The following hostnames comply with Section 2.1 of RFC 1123:

- Name.Example.COM
- XX
- 3.example.org
- 4-.5.9.1.6.US

The following hostnames do not comply with Section 2.1 of RFC 1123:

– Name.Example.a	The TLD “a” is too short.

– Name.-e.com	A label cannot start with “-”.
– Name_Example.Example.COM	“_” is not a valid character.
– Name.Example..com	A label must be at least one character.
– Example.com.	A label must be at least one character.

When the **ip hostname strict** command is configured on a router, any hostname configured on the router must comply with Section 2.1 of RFC 1123, including the following configurations:

- Router(config)# **hostname router1**
- Router(config)# **ip domain name domainname1.com**
- Router(config)# **ip domain list list1.com**
- Router(config)# **ip host host.example.com 10.0.0.1**
- Router(config)# **ipv6 host a.example.com 1000::1**

When the **ip hostname strict** command is not configured on a router, characters that are not specified in Section 2.1 of RFC 1123 are allowed in hostnames.

Examples

The following example shows how to specify compliance with Section 2.1 of RFC 1123 for hostnames.

```
Router(config)# ip hostname strict
```

Related Commands

Command	Description
hostname	Defines the hostname for a network server.
ip domain list	Defines a list of default domain names to complete unqualified hostnames.
ip domain name	Defines a default domain name to complete unqualified hostnames.
ip host	Defines static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view.
ipv6	Defines a static hostname-to-address mapping in the hostname cache.

ip hp-host

To enter into the host table the host name of a Hewlett-Packard (HP) host to be used for HP Probe Proxy service, use the **ip hp-host** global configuration command. To remove a host name, use the **no** form of this command.

ip hp-host *host-name ip-address*

no ip hp-host *host-name ip-address*

Syntax Description

host-name	Name of the host.
ip-address	IP address of the host.

Defaults

No host names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command is no longer available from Cisco IOS Mainline or Technology-based (T) releases. It may still appear in Cisco IOS S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using this command.

Examples

The following example specifies the name and address of an HP host, and then enables HP Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface fastethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip probe proxy	Enables the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests.

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

no ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

Syntax Description

timers	(Optional) Indicates that you are setting local-area mobility timers.
keepalive	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 5 minutes (300 seconds).
hold-time	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 15 minutes (900 seconds).
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Defaults

Local-area mobility is disabled.

If you enable local-area mobility:
keepalive: 5 minutes (300 seconds)
hold-time: 15 minutes (900 seconds)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be taken for mobile nodes and disrupt normal operations.

Examples

The following example configures local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
 interface fastethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip netmask-format

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

ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}

no ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}

Syntax Description

bit-count	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

Defaults

Netmasks are displayed in dotted-decimal format.

Command Modes

Line configuration

Command History

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

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 10.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 10.108.11.0 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 10.108.11.0/24.

Examples

The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

ip options

To drop or ignore IP options packets that are sent to the router, use the **ip options** command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

ip options {**drop** | **ignore**}

no ip options {**drop** | **ignore**}

Syntax Description

drop	Router drops all IP options packets that it receives.
ignore	Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet—just ignored.) **Note** This option is not available on the Cisco 10000 series router.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(19)	This command was integrated into Cisco IOS Release 12.3(19).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 for the PRE3.

Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and you configure the ignore mode, the ignore mode overrides the drop mode.

Cisco 10720 Internet Router

The **ip options ignore** command is not supported. Only drop mode (the **ip options drop** command) is supported.

Cisco 10000 Series Router

This command is only available on the PRE3. The PRE2 does not support this command.

The **ip options ignore** command is not supported. The router supports only the **ip options drop** command.

Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop

% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
ignore modes.
end
```

ip probe proxy

To enable the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests, use the **ip probe proxy** interface configuration command. To disable HP Probe Proxy, use the **no** form of this command.

ip probe proxy

no ip probe proxy

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command is no longer available from Cisco_IOS Mainline or Cisco_IOS Technology-based (T) releases. It may continue to appear in Cisco_IOS S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

HP Probe Proxy Name requests are typically used at sites that have Hewlett-Packard (HP) equipment and are already using HP Probe.

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using the **ip hp-host** global configuration command.

Examples

The following example specifies an HP host name and address, and then enables Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface fastethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip hp-host	Enters into the host table the host name of an HP host to be used for HP Probe Proxy service.

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

no ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.

Release	Modification
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network** (DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>

router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ```

  RIP and EIGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

  ```
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

- EIGRP redistributes the route with both of the following commands:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, **ip route 0.0.0.0 0.0.0.0 ethernet 1**/**2 10.1.2.3**) with a static route to prevent routes from passing through an unintended interface.

Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**, displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config | include ip route

ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route vrf

To establish static routes for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

Supported Static Route Configurations

When you configure static routes in a Multiprotocol Label Switching (MPLS) or MPLS VPN environment, note that some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS releases 12.*x*T, 12.*x*M, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1**
ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1**
ip route *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

- – **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- – **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- – **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**
  ip route vrf *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet gateway.

- – **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- – **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  (This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1**
ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global**
ip route vrf *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1**
ip route vrf *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (EBGP) multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1**
ip route *destination-prefix mask* **interface2 nexthop2**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
redistribute static	Redistributes routes from another routing domain into the specified domain.

ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no** form of this command.

ip routing

no ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

Examples

The following example enables IP routing:

```
ip routing
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *type mod*/*port*

Syntax Description

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

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

Examples

This example shows how to add a static IP source binding entry:

```
Router(config)# ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface
gigabitethernet5/3
```

This example shows how to delete a static IP source binding entry:

```
Router(config)# no ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface
gigabitethernet5/3
```

Related Commands

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

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Examples

The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** command in global configuration mode. To restore the default, use the **no** form of this command.

ip subnet-zero

no ip subnet-zero

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ip subnet-zero** command provides the ability to configure and route to subnet 0 subnets.

Subnetting with a subnet address of 0 is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

Examples

The following example enables subnet zero:

```
ip subnet-zero
```

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number*

no ip unnumbered *type number*

Syntax Description

type	Interface on which the router has assigned an IP address. The interface cannot be unnumbered interface. 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

IP processing on the unnumbered interface is disabled.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command became available on the Supervisor Engine 720.
12.2(18)SXF	This command was modified to support Ethernet physical interfaces and switched virtual interfaces (SVIs).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When an unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

- This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and ‘*number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.

Note Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, any routing protocol running across the serial line must not advertise subnet information.

Examples

In the following example, the first serial interface is given the address of Ethernet 0:

```
interface fastethernet 0
 ip address 10.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered fastethernet 0
```

In the following example, Ethernet VLAN subinterface 3/0.2 is configured as an IP unnumbered subinterface:

```
interface fastethernet 3/0.2
 encapsulation dot1q 200
 ip unnumbered fastethernet 3/1
```

In the following example, Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 are configured as IP unnumbered subinterfaces:

```
interface range fastethernet5/1.1 - fastethernet5/1.4
 ip unnumbered fastethernet 3/1
```

ip verify source vlan dhcp-snooping

To enable Layer 2 IP source guard, use the **ip verify source vlan dhcp-snooping** command in the service instance mode. Use the **no** form of this command to disable Layer 2 IP source guard.

ip verify source vlan dhcp-snooping [**port-security**]

no ip verify source vlan dhcp-snooping [**port-security**]

Syntax Description

port-security	Enables IP/MAC mode and applies both IP and MAC filtering.

Command Default

Layer 2 IP source guard is disabled.

Command Modes

Service instance (config-if-srv)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **port-security** keyword was added.

Usage Guidelines

The **ip verify source vlan dhcp-snooping** command enables VLANs only on the configured service instance (EVC) and looks for DHCP snooping matches only for the configured bridge domain VLAN.

Examples

This example shows how to enable Layer 2 IP source guard on an interface:

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 fastethernet
Router(config-if-srv)# encapsulation dot1q 71
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# ip verify source vlan dhcp-snooping
Router(config-if-srv)#  bridge-domain 10
```

Related Commands

Command	Description
service instance ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

local-ip (IPC transport-SCTP local)

To define at least one local IP address that is used to communicate with the local peer, use the **local-ip** command in IPC transport-SCTP local configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

local-ip *device-real-ip-address* [*device-real-ip-address2*]

no local-ip *device-real-ip-address* [*device-real-ip-address2*]

Syntax Description

device-real-ip-address	IP address of the local device. The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
device-real-ip-address2	(Optional) IP address of the local device.

Defaults

No IP addresses are defined; thus, peers cannot communicate with the local peer.

Command Modes

IPC transport-SCTP local configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **local-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switchover (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port number that is used to communicate with the redundant peer.
remote-ip	Defines at least one remote IP address that is used to communicate with the redundant peer.

local-port

To define the local Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **local-port** command in SCTP protocol configuration mode.

local-port *local-port-number*

Syntax Description

local-port-number	Local port number, which should be the same as the remote port number on the peer router (which is specified via the **remote-port** command).

Defaults

A local SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **local-port** command enters IPC transport-SCTP local configuration mode, which allows you to specify at least one local IP address (via the **local-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-ip (IPC transport-SCTP remote)

To define at least one IP address of the redundant peer that is used to communicate with the local device, use the **remote-ip** command in IPC transport-SCTP remote configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]

no remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]

Syntax Description

peer-real-ip-address	IP address of the remote peer. The remote IP addresses must match the local IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
peer-real-ip-address2	(Optional) IP address of the remote peer.

Defaults

No IP addresses are defined.

Command Modes

IPC transport-SCTP remote configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **remote-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switch Over (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-port

To define the remote Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **remote-port** command in SCTP protocol configuration mode.

remote-port *remote-port-number*

Syntax Description

remote-port-number	Remote port number, which should be the same as the local port number on the peer router (which is specified via the **local-port** command).

Defaults

A remote SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **remote-port** command enters IPC transport-SCTP remote configuration mode, which allows you to specify at least one remote IP address (via the **remote-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.

show hosts

To display 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 Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

show hosts [**vrf** *vrf-name*] [**view** *view-name*] [**all** | *hostname*] [**summary**]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
all	(Optional) The specified hostname cache information is to be displayed for all configured DNS views. This is the default.
hostname	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was updated to support the Cisco modem user interface feature.
12.4(4)T	The **vrf**, **all**, and **summary** keywords and *vrf-name* and *hostname* arguments were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command 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.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Examples

The following is sample output from the **show hosts** command with no parameters specified:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
user                      None  (perm, OK)   0   IP   192.0.2.001
www.example.com           None  (perm, OK)   0   IP   192.0.2.111
                                                      192.0.2.112
```

Table 23 describes the significant fields shown in the display.

Table 23 show hosts Field Descriptions

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.

Table 23 show hosts Field Descriptions (continued)

Field	Description
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the **ip hosts** command.
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: • temp—A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. • perm—A permanent entry is entered by a configuration command and is not timed out. • OK—Entries marked OK are believed to be valid. • ??—Entries marked ?? are considered suspect and subject to revalidation. • EX—Entries marked EX are expired.
Age	Number of hours since the software last referred to the cache entry.
Type	Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the **ip hp-host global** configuration command, the **show hosts** command will display these hostnames as type HP-IP.
Address(es)	IP address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

show ip aliases

To display the IP addresses mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the “port” number, where 1 is the auxiliary port.

Examples

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

```
Router# show ip aliases

 IP Address    Port
10.108.29.245 SLIP TTY1
```

The display lists the IP address and corresponding port number.

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was expanded to include the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.

Usage Guidelines

The Cisco IOS software automatically enters a directly-connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly-connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface. If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to view a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information on interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3

interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBR_NAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3

GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, “Downstream VPN Routing/Forwarding “D”” identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3

Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3

Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
```

```
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled
```

Table 24 describes the significant fields shown in the display.

Table 24 show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.

Table 24 show ip interface Field Descriptions (continued)

Field	Description
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding (CEF) switching is enabled for the interface.
Downstream VPN Routing/Forwarding “D”	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Shows whether NetFlow is enabled on an interface. Displays “Flow init” to specify that NetFlow is enabled on the interface. Displays “Ingress Flow” to specify that NetFlow is enabled on a subinterface using the **ip flow ingress** command. Shows “Flow” to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief

Interface      IP-Address      OK?  Method  Status                   Protocol
Ethernet0      10.108.00.5     YES  NVRAM   up                       up
Ethernet1      unassigned      YES  unset   administratively down    down
Loopback0      10.108.200.5    YES  NVRAM   up                       up
Serial0        10.108.100.5    YES  NVRAM   up                       up
Serial1        10.108.40.5     YES  NVRAM   up                       up
Serial2        10.108.100.5    YES  manual  up                       up
Serial3        unassigned      YES  unset   administratively down    down
```

Table 25 describes the significant fields shown in the display.

Table 25 show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is currently valid. "No" means that the IP Address is not currently valid.
Method	The Method field has the following possible values: • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP—Bootstrap protocol. • TFTP—Configuration file obtained from the TFTP server. • manual—Manually changed by CLI command. • NVRAM—Configuration file in NVRAM. • IPCP—**ip address negotiated** command. • DHCP—**ip address dhcp** command. • unassigned—No IP address. • unset—Unset. • other—Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
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 route-map	Displays static and dynamic route maps.

show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** command in EXEC mode.

show ip irdp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
 --More--
Serial 0 has router discovery disabled
 --More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

```
Advertisements will occur between every 450 and 600 seconds.
```

This indicates the configured minimum and maximum advertising interval for the interface.

```
Advertisements are valid for 1800 seconds.
```

This indicates the configured holdtime values for the interface.

```
Default preference will be 100.
```

This indicates the configured (or in this case default) preference value for the interface.

Related Commands

Command	Description
ip irdp	Enables IRDP processing on an interface.

show ip masks

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

show ip masks *address*

Syntax Description

address	Network address for which a mask is required.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ip masks 172.16.0.0

Mask            Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download** | **update-queue**]

Syntax Description

ip-address	(Optional) IP address about which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocl (NHRP) overrides associated with a particular route, along with the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) The subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
protocol	(Optional) The name of a routing protocol, or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhr**, and **rip**.
process-id	(Optional) The number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Specific access list number for which output from the routing table should be displayed.
access-list-name	(Optional) Specific access list name for which output from the routing table should be displayed.
static	(Optional) Displays static routes.
download	(Optional) Displays the route installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
11.1	The “U—per-user static route” code was added to the command output.
11.2	The “o—on-demand routing” code was added to the command output.
12.2(33)SRA	This command was modified. The **update-queue** keyword was added.
11.3	The output from the **show ip route** *ip-address* command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The “M—mobile” code was added to the command output.
12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
12.0(4)T	The “ia—IS-IS” code was added to the command output.
12.2(2)T	The output from the **show ip route** *ip-address* command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The *egp* and *igrp* arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	The output was enhanced to display route tag information.
12.3(8)T	The output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was modified. The **dhcp** and **repair-paths** keywords were added. Support for the Border Gateway Protocol (BGP) best external and BGP additional path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was modified. The **next-hop-override** and **nhrp** keywords were added.

Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

Examples

Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in Table 28 to understand the type of route.

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

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: L- Local R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 192.168.1.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         10.10.10.0/24 is directly connected, Vlan1
L         10.10.10.1/32 is directly connected, Vlan1
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.1.0/30 is directly connected, GigabitEthernet0
L         192.168.1.1/32 is directly connected, GigabitEthernet0
```

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: L - Local R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.4.9.0/24 is directly connected, GigabitEthernet0/1
L        10.4.9.134/32 is directly connected, GigabitEthernet0/1
      171.69.0.0/16 is variably subnetted, 2 subnets, 2 masks
S        171.69.0.0/16 [1/0] via 10.4.9.1
S        171.69.1.129/32 [1/0] via 10.4.9.1
```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Router# show ip route static

     172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
```

```
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to display all active and inactive routes installed using AAA route download:

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following example shows how to use the **show ip route nhrp** command to enable shortcut switching on the tunnel interface:

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP

Gateway of last resort is not set

       10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following is sample output using the **next-hop-override** keyword. When the **next-hop-override** keyword is included, the NHRP Nexthop-overrides associated with a particular route, along with the corresponding default next hops, are displayed.

```
===============================================================
1) Initial configuration
===============================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
127.0.0.0/8          drop
.
.
.
===============================================================
2) Add a Nexthop-override
    address = 10.10.10.0
    mask = 255.255.255.0
    gateway = 10.1.1.1
    interface = Tunnel0
===============================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```
Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
% S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
% S        10.10.10.0 is directly connected, Tunnel0
                    [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24       10.1.1.1             Tunnel0
10.11.11.0/24       attached           Ethernet0/0
10.12.0.0/16 drop
.
.
.

===============================================================
3) Delete a Nexthop-override
    address = 10.10.10.0
    mask = 255.255.255.0
    gateway = 10.11.1.1
    interface = Tunnel0
===============================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```
Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

Table 26 show ip route Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H— NHRP • i—IS-IS derived • ia—IS-IS • L—local • M—mobile • O—Open Shortest Path First (OSPF) derived • P—periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—static • U—per-user static route • o—on-demand routing • +—replicated route
Codes	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF inter area route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via “isis”, distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

Table 29 describes the significant fields shown when using the **show ip route** command with an IP address.

Table 27 show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via “isis”, distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows the repair paths marked with the tag [RPR]:

```
Router# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Router# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Table 28 show ip route Field Descriptions

Field	Description
O	Indicates the protocol that derived the route. It can be one of the following values: R—Routing Information Protocol (RIP) derived O—Open Shortest Path First (OSPF) derived C—connected S—static B—Border Gateway Protocol (BGP) derived D—Enhanced Interior Gateway Routing Protocol (EIGRP) EX—EIGRP external i—IS-IS derived ia—IS-IS M—mobile P—periodic downloaded static route U—per-user static route o—on-demand routing
E2	Type of route. It can be one of the following values: *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. IA—OSPF interarea route E1—OSPF external type 1 route E2—OSPF external type 2 route L1—IS-IS Level 1 route L2—IS-IS Level 2 route N1—OSPF not-so-stubby area (NSSA) external type 1 route N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.

Table 28 show ip route Field Descriptions (continued)

Field	Description
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The example above shows the output from the **show ip route** command when looking at an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

Table 29 describes the significant fields shown when using the **show ip route** command with an IP address.

Table 29 show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.

Table 29 show ip route with IP Address Field Descriptions (continued)

Field	Description
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via “isis”, distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows the repair paths marked with the tag [RPR]:

```
Router# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
```

```
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Router# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip source binding

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

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

Syntax Description

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

Command Default

Both static and DHCP-snooping bindings are displayed.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Each optional parameter is used to filter the display output.

Examples

This example shows the output without entering any keywords:

```
Router# show ip source binding

MacAddress              IpAddress        Lease(sec) Type          VLAN Interface
------------------      --------------- ---------- ------------- ---- --------------------
00:00:00:0A:00:0B       17.16.0.1         infinite   static        10   FastEthernet6/10
00:00:00:0A:00:0A       17.16.0.2         10000      dhcp-snooping 10   FastEthernet6/11
```

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

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

Table 30 describes the significant fields in the display.

Table 30 show ip source binding Field Descriptions

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

Related Commands

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

show ip verify source

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

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ip verify source interface gigabitethernet6/1

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                    11-20
```

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

```
Router# show ip verify source interface gigabitethernet6/1

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           inactive-trust-port
```

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

```
Router# show ip verify source interface gigabitethernet6/3
```

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/3      ip           inactive-no-snooping-vlan
```

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

```
Router# show ip verify source interface gigabitethernet6/4

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

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

```
Router# show ip verify source interface gigabitethernet6/5

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
```

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

```
Router# show ip verify source interface gigabitethernet6/6

DHCP security is not configured on the interface gi6/6.
```

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

```
Router# show ip verify source

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

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

```
Router# show ip verify source interface gi5/0/0 efp_id 10

Interface  Filter-type  Filter-mode  IP-address       Mac-address       Vlan        EFP
ID
---------    -----------    -----------      ---------------     -----------------
----------  ----------
Gi5/0/0    ip-mac       active          123.1.1.1        00:0A:00:0A:00:0A  100        10
Gi5/0/0    ip-mac       active          123.1.1.2        00:0A:00:0A:00:0B  100        20
Gi5/0/0    ip-mac       active          123.1.1.3        00:0A:00:0A:00:0C  100        30
```

Related Commands

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

term ip netmask-format

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

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

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

Syntax Description

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

Defaults

Netmasks are displayed in dotted decimal format.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

NAT Commands

application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode**.**

application redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

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

Examples

The following example shows how to enter redundancy application configuration mode:

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

Related Commands

Command	Description
group	Enters redundancy application group configuration mode.

authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication** command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

no authentication {**text** *string* | **md5 key-string** [**0** | **7**] *key* | **md5 key-chain** *key-chain-name*}

Syntax Description

text *string*	Uses clear text authentication.
md5 key-string	Uses MD5 key authentication. The *key* argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
0	(Optional) Specifies that the the text following immediately is not encrypted.
7	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
md5 key-chain *key-chain-name*	Uses MD5 key-chain authentication.

Command Default

The key is not encrypted.

Command Modes

Redundancy application group protocol configuration (config-red-app-prtcl)

Command History

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

Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# authentication text name1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in EXEC mode.

clear ip nat translation {*** | forced | [piggyback-internal | esp** | **tcp** | **udp**] [**inside** *global-ip* [*global-port*] *local-ip* [*local-port*] **outside** *local-ip global-ip*] | **inside** *global-ip local-ip* [**forced**] | **outside** *local-ip global-ip* [**forced**]}

Syntax Description

*****	Clears all dynamic translations.
forced	(Optional) Forces the clearing of either: • all dynamic entries, whether or not there are any child translations. • a single dynamic half-entry and any existing child translations, whether or not there are any child translations.
piggyback-internal	(Optional) Clears translations created off of piggyback data.
esp	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
tcp	(Optional) Clears the TCP entries from the translation table.
udp	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.
inside	(Optional) Clears the inside translations containing the specified *global-ip* and *local-ip* addresses. If used without the **forced** keyword, clears only those entries that do not have child translations.
global-ip	(Optional) Global IP address.
global-port	(Optional) Global port.
local-ip	(Optional) Local IP address.
local-port	(Optional) Local port.
outside	(Optional) Clears the outside translations containing the specified *global* and *local* addresses. If used without the **forced** keyword, clears only those entries that do not have child translations.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The **esp** keyword was added.
12.4(2)T	The **piggyback-internal** keyword was added.
12.2 (33) XND	The **forced** keyword was extended to support the removal of a half entry regardless of whether it has any child translations.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.4.2	The **forced** keyword was extended for Cisco IOS XE Release 2.4.2 to support the removal of a half entry regardless of whether it has any child translations.
15.0(1)M2	The **forced** keyword was extended for Cisco IOS release 15.0(1)M2 to support the removal of a half entry regardless of whether it has any child translations.

Usage Guidelines

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

Examples

The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router> show ip nat translations

Pro    Inside global        Inside local       Outside local      Outside global
udp    10.69.233.209:1220  10.168.1.95:1220   10.69.2.132:53     10.69.2.132:53
tcp    10.69.233.208       10.168.1.94
tcp    10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp    10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23

Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
outside 10.69.2.132 53 10.69.2.132 53

Router# show ip nat translations

Pro     Inside global       Inside local       Outside local      Outside global
tcp     10.69.233.208       10.168.1.94
tcp     10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp     10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23

Router# clear ip nat translation inside 10.69.233.208 10.168.1.94 forced

Router# show ip nat translations

Pro     Inside global       Inside local       Outside local      Outside global
tcp     10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp     10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23
```

Related Commands

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

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 stateless prefix.

Examples

The following example shows how to clear NAT64 statistics:

```
Router# clear nat64 statistics
```

Related Commands

Command	Description
show nat64 statistics	Displays statistics about NAT64 interfaces and the translated and dropped packet count.

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 control interface for the redundancy group, use the **no** form of this command.

control *interface-name number* **protocol** *id*

no control

Syntax Description

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

Command Default

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 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.
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	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-name number*

no data *interface-name number*

Syntax Description

interface-name	Interface name.
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. 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.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

Command	Description
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

debug redundancy application group config

To display the redundancy application group configuration, use the **debug redundancy application group config** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group config {**all** | **error** | **event** | **func**}

no debug redundancy application group config {**all** | **error** | **event** | **func**}

Syntax Description

all	Displays debug information about configuration.
error	Displays information about the redundancy group's configuration errors.
event	Displays information about the redundancy group's configuration .
func	Displays information about the redundancy group's configuration functions entered.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# debug redundancy application group config all

RG config all debugging is on
```

Related Commands

Command	Description
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group RII	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.
debug redundancy application group VP	Displays the redundancy application group VP information.

debug redundancy application group faults

To display the redundancy application group faults, use the **debug redundancy application group faults** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group faults {**all** | **error** | **event** | **fault** | **func**}

no debug redundancy application group faults {**all** | **error** | **event** | **fault** | **func**}

Syntax Description

all	Displays fault information of a redundancy group.
error	Displays error information of a redundancy groups.
event	Displaysevent information of a redundancy group.
fault	Displays fault events information of a redundancy group.
func	Displays fault functions information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **debug redundancy application group faults error** command:

```
Router# debug redundancy application group faults error

RG Faults error debugging is on
```

Related Commands

Command	Description
redundancy application group config	display the redundancy application group configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.

Command	Description
debug redundancy application group transport	Displays the redundancy group application group transport information.
debug redundancy application group vp	Displays the redundancy group application group VP information.

debug redundancy application group media

To display the redundancy application group media information, use the **debug redundancy application group media** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group media {**all** | **error** | **event** | **nbr** | **packet** {**rx** | **tx**} **| timer**}

no debug redundancy application group media {**all** | **error** | **event** | **nbr** | **packet** {**rx** | **tx**} **| timer**}

Syntax Description

all	Displays media information of a redundany group.
error	Displays media errors information of a redundany group.
event	Displays media events information of a redundany group.
nbr	Displays media neighbor (nbr) information of a redundany group.
packet	Displays media packets information of a redundany group.
rx	Displays the incoming packets information.
tx	Displays the outgoing packets information.
timer	Displays media timer events information about redundancy group media timer events.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **debug redundancy application group media timer** command:

```
Router# debug redundancy application group media timer

RG Media timer debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy group application group protocol information.
debug redundancy application group rii	Displays the redundancy group application group RII information.

Command	Description
debug redundancy application group transport	Displays the redundancy group application group transport information.
debug redundancy application group vp	Displays the redundancy application group VP information.
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group protocol

To display the redundancy application group protocol information, use the **debug redundancy application group protocol** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group protocol {**all** | **detail** | **error** | **event** | **media** | **peer**}

no debug redundancy application group protocol {**all** | **detail** | **error** | **event** | **media** | **peer**}

Syntax Description

all	Displays protocol information of a redundancy group.
detail	Displays event details of a redundancy group.
error	Displays protocol error information of a redundancy group.
event	Displays protocol events information of a redundancy group.
media	Displays protocol media events information of a redundancy group.
peer	Displays protocol peer information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **debug redundancy application group protocol peer** command:

```
Router# debug redundancy application group protocol peer

RG Protocol peer debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.

Command	Description
debug redundancy application group vp	Displays the redundancy application group VP information.
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
redundancy application group config	Displays the redundancy application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group rii

To display the redundancy application group RII information, use the **debug redundancy application group rii** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group rii {**error** | **event**}

no debug redundancy application group rii {**error** | **event** }

Syntax Description

error	Displays RII errors information about the redundancy group's .
event	Dispalys information about the redundancy group's RII events.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **debug redundancy application group rii event** command:

```
Router# debug redundancy application group rii event

RG RII events debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy group application group protocol information.
debug redundancy application group rii	Displays the redundancy group application group RII information.
debug redundancy application group vp	Displays the redundancy group application group VP information.
redundancy application group config	Displays the redundancy group application configuration.

Command	Description
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group transport

To display the redundancy application group transport information, use the **debug redundancy application group transport** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group transport {**db** | **error** | **event** | **packet** | **timer** | **trace**}

no debug redundancy application group transport {**db** | **error** | **event** | **packet** | **timer** | **trace**}

Syntax Description

db	Displays transport information of a redundancy group.
error	Displays ransport error information of a redundancy group.
event	Displays transport event information of a redundancy group.
packet	Displays transport packet information of a redundancy group.
timer	Displays transport timer information of a redundancy group.
trace	Displays transport trace information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# debug redundancy application group transport trace


RG Transport trace debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group vp

To display the redundancy application group virtual platform (VP) information, use the **debug redundancy application group VP** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug redundancy application group vp {**error** | **event**}

no debug redundancy application group vp{**error** | **event**}

Syntax Description

error	Displays VP errors information of a redundancy group.
event	Displays VP event information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **debug redundancy application group vp event** command:

```
Router# debug redundancy application group vp event

RG VP events debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.
redundancy application group config	Displays the redundancy application configuration.
debug redundancy application group media	Displays the redundancy application group media information.

Command	Description
debug redundancy application group protocol	Displays the redundancy application group protocol information.
redundancy application group config	Displays the redundancy application configuration.

group

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 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.

ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), to enable NAT logging, or to enable static IP address support, use the **ip nat** command in interface configuration mode. To prevent the interface from being able to translate or log, use the **no** form of this command.

ip nat [**inside** | **outside** | **Stateful** | **create** | **piggyback-support** | **pool** | **portmap** | **service** | **sip-sbc** | **source** | **log** | **translations** | **syslog** | **allow-static-host**]

no ip nat [**inside** | **outside** | **Stateful** | **create** | **piggyback-support** | **pool** | **portmap** | **service** | **sip-sbc** | **source** | **log** | **translations** | **syslog** | **allow-static-host**]

Syntax Description

allow-static-host	(Optional) Enables static IP address support for NAT translation.
create	(Optional) Creates NAT flow entries.
inside	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
log	(Optional) Enables NAT logging.
outside	(Optional) Indicates that the interface is connected to the outside network.
piggyback-support	(Optional) Enables NAT Piggybacking support.
pool	(Optional) Defines pool of addresses.
portmap	(Optional)Defines portmap of portranges.
service	(Optional) Indicates special translation for application using non-standard port.
sip-sbc	(Optional) Indicates SIP Session Border Controller commands.
source	(Optional)
Stateful	(Optional)
syslog	(Optional) Enables syslog for NAT logging translations.
translations	(Optional) Enables NAT logging translations.

Command Default

Traffic leaving or arriving at this interface is not subject to NAT.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The **allow-static-host** keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command is integrated into the Cisco IOS Release 12.2(22)T. The **allow-static-host** keyword was removed.

ip nat create flow-entries

To create Network Address Translation (NAT) flow entries, use the **ip nat create** command in global configuration mode. To disable the flow cache, use the **no** form of this command.

ip nat create flow-entries

no ip nat create flow-entries

Syntax Description

This command has no arguments or keywords.

Command Default

Flow entries are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

To scale the performance of NAT, an enhancement is created that allows for a flow table for NAT entries.

Examples

The following example shows how to create NAT flow entries:

```
Router(config)# no ip nat create flow-entries
```

Related Commands

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

ip nat enable

To configure an interface connecting Virtual Private Networks (VPNs) and the Internet for Network Address Translation (NAT), use the **ip nat enable** command in interface configuration mode.

ip nat enable

no ip nat enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

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

Examples

The following example show how to configure an interface connecting VPNs and the Internet for NAT translation:

```
interface Ethernet0/0
 ip vrf forwarding vrf1
 ip address 192.168.122.1 255.255.255.0
 ip nat enable
```

Related Commands

Command	Description
ip nat pool	Defines a pool of IP addresses for Network Address Translation.
ip nat source	Enables Network Address Translation on a virtual interface without inside or outside specification.

ip nat inside destination

To enable the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination** command in global configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. To remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside destination list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

no ip nat inside destination list {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated during dynamic translation.
mapping-id *map-id*	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

Defaults

No inside destination addresses are translated.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	The **mapping-id** *map-id* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To implement TCP load balancing, you must configure NAT to use rotary pools as specified with the **ip nat pool** command and the **rotary** keyword.

Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

For more information about implementing TCP load balancing, see the *Cisco IOS IP Addressing Services Configuration Guide*.

Examples

The following example shows how to define a virtual address with connections that are distributed among a set of real hosts. The rotary pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose destination matches the access list are translated to an address from the rotary pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0/0/0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface GigabitEthernet 0/0/1
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

Related Commands

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

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation, or the dynamic association to a pool, use the **no** form of this command.

Dynamic NAT

ip nat inside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**no-payload**] [**overload**] [**reversible**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]

no ip nat inside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**no-payload**] [**overload**] [**reversible**] [**vrf** *name* [**match-in-vrf**]] [**oer**] [**portmap** *name*]

Static NAT

ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]]

no ip nat inside source static {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*} [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]]

Port Static NAT

ip nat inside source static {{**tcp** | **udp**} {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}}

no ip nat inside source static {**tcp** | **udp** {*local-ip local-port global-ip global-port* [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**route-map** *name* [**reversible**]] [**vrf** *name* [**match-in-vrf**]] | **interface** *global-port*}}

Network Static NAT

ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**vrf** *name* [**match-in-vrf**]]

no ip nat inside source static network *local-network global-network mask* [**extendable**] [**forced**] [**mapping-id** *map-id*] [**no-alias**] [**no-payload**] [**redundancy** *group-name*] [**vrf** *name* [**match-in-vrf**]]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.

route-map *name*	Specifies the named route map.
interface	Specifies an interface for the global address.
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.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated dynamically.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
reversible	(Optional) Enables outside-to-inside initiated sessions to use route maps for destination-based NAT.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
oer	(Optional) Allows Optimized Edge Routing (OER) to operate NAT and control traffic class routing.
portmap *name*	(Optional) Specifies the portmap to be associated for NAT.
static	Sets up a single static translation.
esp *local-ip*	Establishes the IPsec Encapsulating Security Payload (ESP) (tunnel mode) support.
local-ip	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
global-ip	Globally unique IP address of an inside host as it appears to the outside network.
extendable	(Optional) Extends the translation.
forced	(Optional) Forcefully deletes an entry and its children from the configuration.
mapping-id *map-id*	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
no-alias	(Optional) Prohibits an alias from being created for the global address.
redundancy *group-name*	(Optional) Establishes NAT redundancy.
tcp	Establishes the TCP protocol.
udp	Establishes the UDP protocol.
local-port	Local TCP or UDP port in a range from 1 to 65535.
global-port	Global TCP or UDP port in a range from 1 to 65535.
network *local-network*	Specifies the local subnet translation.
global-network	Global subnet translation.
mask	IP network mask to be used with subnet translations.

Command Default

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the **route-map** *name* keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	This command was modified. The **interface** keyword was added for static translations. The **vrf** *name* keyword and argument combination was added.
12.3(7)T	This command was modified. The static **mapping-id** *map-id* keyword and argument combination was added.
12.4(3)T	This command was modified. The **reversible** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified. The **oer** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword and argument pair was removed from Cisco 7600 series routers.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The optional keywords of the **ip nat inside source** command can be entered in any order.

For information about the limitations when the **ip nat inside source** command was integrated into Cisco IOS XE Release 2.5, see the *Cisco IOS XE 2 Release Notes*.

This command has two forms: the dynamic and the static address translation. The form with an access list establishes the dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Note When a session is initiated from outside with the source IP as the outside global address, the router is unable to determine the destination VRF of the packet. Use the **match-in-vrf** keyword to enable the IP alias installation to work correctly when routing NAT inside and outside traffic in the same VRF.

Examples

The following example shows how to translate between inside hosts addressed from either the 192.0.2.0 or the 198.51.100.0 network to the globally unique 203.0.113.209/28 network:

```
ip nat pool net-209 203.0.113.209 203.0.113.222 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 203.0.113.113 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.0.2.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.0.2.1 255.255.255.0
access-list 1 permit 198.51.100.253 255.255.255.0
```

The following example shows how to translate the traffic that is local to the provider's edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface ethernet 0 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 0 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 192.0.2.1
ip route vrf vrf2 10.0.0.1 10.0.0.1 192.0.2.1
!
access-list 1 permit 10.1.1.1 0.0.0.255
!
ip nat inside source list 1 interface ethernet 1 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 1 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 198.51.100.1 global
ip route vrf vrf2 10.0.0.1 10.0.0.1 198.51.100.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

The following example shows how to translate sessions from outside-to-inside:

```
ip nat pool POOL-A 10.1.10.1 10.1.10.126 255.255.255.128
ip nat pool POOL-B 10.1.20.1 10.1.20.126 255.255.255.128

ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 10.1.20.128 0.0.0.127
!
route-map MAP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B
!
```

The following example shows how to configure the route map R1 to allow outside-to-inside translation for static NAT:

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127

route-map R1 permit 10
```

```
 match ip address ACL-A
```

The following example shows how to configure NAT inside and outside traffic in the same VRF:

```
interface Loopback1
 ip vrf forwarding forwarding1
 ip address 192.0.2.11 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip vrf forwarding forwarding2
 ip address 192.0.2.22 255.255.255.0
 ip nat outside
 ip virtual-reassembly

ip nat pool MYPOOL 192.0.2.5 192.0.2.5 prefix-length 24
ip nat inside source list acl-nat pool MYPOOL vrf vrf1 overload
!
!
ip access-list extended acl-nat
 permit ip 192.0.2.0 0.0.0.255 any
```

Related Commands

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

ip nat log translations flow-export

To enable high speed logging for all or some a Network Address Translation (NAT) translations, use the **ip nat log translations flow-export** command in global configuration mode. To remove one or more translations from the log, use the **no** form of this command.

ip nat log translations flow-export v9 {**udp destination** *addr port* **source** *interface interface-number* | {*vrf-name* | **global-on**}}

no ip nat log translations flow-export v9 {**udp destination** *addr port* **source** *interface interface-number* | {*vrf-name* | **global-on**}}

Syntax Description

destination *addr port*	Specifies the destination address for which translations will be logged.
source *interface interface-number*	Specifies the source interface for which translations will be logged.
vrf-name	Specifies the Virtual Private Network (VPN) for which translations will be logged. The VPN is identified by the VPN Routing and Forwarding (VRF) network name.
global-on	Enables high speed logging for all Virtual Private Networks (VPNs).

Command Default

Logging is disabled for all translations

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You must first use the **ip nat log translations flow-export v9 udp destination** command to enable high speed logging for all VPN and non-VPN translations. VPN translations are also know as VPN Routing and Forwarding (VRF) translations.

After you enable high speed logging for all NAT translations, you can then use the **ip nat log translations flow-export v9** *vrf-name* command to enable or disable translations for specific VPNs. When you use this command, high speed logging is disabled for all VPNs except for the ones where it is explicitly enabled.

Examples

The following example shows how to enable logging for a specific VPN.

```
Router(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020
source Ethernet 0/0
Router(config)# ip nat log translations flow-export v9 VPN-18
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Enables NAT of the outside source address.
show ip nat translations	Displays active NAT translations.

ip nat log translations syslog

To define a set of log translations for Network Address Translation (NAT), use the **ip nat log** command in global configuration mode. To remove one or more translations from the log, use the **no** form of this command.

ip nat log translations syslog

no ip nat log translations syslog

Syntax Description

translations	Enables the NAT logging translations.
syslog	Enables the writing of NAT log to syslog.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to define a set of log translations.

```
Router(config)# ip nat log translations syslog
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Enables NAT of the outside source address.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

Dynamic NAT

ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route** | **mapping-id** *map-id* | **vrf** *name*]

no ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route** | **mapping-id** *map-id* | **vrf** *name*]

Dynamic NAT for inter-chassis redundancy

ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route**]

no ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route**]

Static NAT

ip nat outside source static *global-ip local-ip* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

no ip nat outside source static *global-ip local-ip* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

Static NAT for inter-chassis redundancy

ip nat outside source static *global-ip local-ip* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

no ip nat outside source static *global-ip local-ip* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

Port Static NAT

ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

no ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

Port Static NAT for inter-chassis redundancy

ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

no ip nat outside source static {**tcp** | **udp**} *global-ip global-port local-ip local-port* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

Network Static NAT

ip nat outside source static network *global-network local-network mask* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** | **vrf** *name*]

no ip nat outside source static network *global-network local-network mask* [**add-route** | **extendable** | **mapping-id** *map-id* **no-alias** | **no-payload** | **redundancy** | **vrf** *name*]

Network Static NAT for inter-chasis redundancy

ip nat outside source static network *global-network local-network mask* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

no ip nat outside source static network *global-network local-network mask* **vrf** *name* **redundancy** *group-ID* **mapping-id** *map-id* [**add-route** | **extendable** | **no-alias** | **no-payload**]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map *name*	Specifies a named route map.
pool *pool-name*	Specifies the name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.
mapping-id *map-id*	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
vrf *name*	(Optional) Associates the NAT translation rule with a particular Virtual Private Network (VPN).
static	Sets up a single static translation.
global-ip	Specifies the globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from globally routable network space.
local-ip	Specifies the local IP address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
global-port	Specifies the port number assigned to a host on the outside network by its owner.
local-port	Specifies the port number of an outside host as it appears to the inside network.
static network	Sets up a single static network translation.
global-network	Specifies the globally unique network address assigned to a host on the outside network by its owner. The address was allocated from globally routable network space.

local-network	Specifies the local network address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside.
mask	Subnet mask for the networks that will be translated.
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the local address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy *group-name*	(Optional) Enables the NAT redundancy operation.
tcp	Establishes the Transmission Control Protocol (TCP).
udp	Establishes the User Datagram Protocol (UDP).

Defaults

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the **redundancy** *group-name* keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the **no-payload** keyword was added.
12.2(13)T	The **mapping-id** *map-id* keyword and argument combination was added for dynamic translations. The **vrf** *name* keyword and argument combination was added.
12.3(7)T	The **mapping-id** *map-id* keyword and argument combination was added for static translations.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For information about the limitations when this command was integrated into Cisco IOS XE Release 2.5, see the *Cisco IOS XE 2 Release Notes*.

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this command if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two general forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

Examples

The following example shows how to translate between inside hosts addressed from the 10.114.11.0 network to the globally unique 10.69.233.208/28 network. Further packets from outside hosts addressed from the 10.114.11.0 network (the true 10.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 10.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.114.11.0 0.0.0.255
```

The following example shows NAT configured on the Provider Edge (PE) router with a static route to the shared service for the group1 and group2 VPNs. NAT is configured as inside source static one-to-one translations.

```
ip nat pool outside 10.4.4.1 10.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 10.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 10.2.2.1 vrf group1
ip nat inside source static 192.169.121.33 10.2.2.2 vrf group2
```

Related Commands

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

ip nat piggyback-support

To enable a Network Address Translation (NAT) optimized Session Initiation Protocol (SIP) media path, use the **ip nat piggyback-support** command in global configuration mode.

ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]

no ip nat piggyback-support sip {**all-messages** | **sdp-only**} **router** *router-id* [**authentication** *authentication-key*]

Syntax Description

sip	SIP protocol algorithm.
all-messages	Establishes piggybacking in all messages except Session Description Protocol (SDP).
sdp-only	Establishes piggybacking in SDP only.
router *router-id*	Piggyback router ID number.
authentication *authentication-key*	(Optional) Specifies the MD5 authentication key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to configure a NAT optimized SIP media path with SDP:

```
ip nat piggyback-support sip sdp-only router 100 authentication md5-key
```

Related Commands

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

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**nopreservation**]

no ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**] [**nopreservation**]

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	Specifies the network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
prefix-length *prefix-length*	Specifies the number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
add-route	(Optional) Specifies that a route has been added to the NAT Virtual Interface (NVI) interface for the global address.
type	(Optional) Indicates the type of pool.
match-host	(Optional) Specifies that the host number is to remain the same after translation.
rotary	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.
accounting *list-name*	(Optional) Indicates the RADIUS profile name that matches the RADIUS configuration in the router.
arp-ping	(Optional) Determines static IP client instances and restarts the NAT entry timer.
nopreservation	(Optional) Enables all the IP addresses in the pool to be used for dynamic translation.

Defaults

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The **accounting** keyword and *list-name* argument were added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	The **add-route** keyword was added.

Release	Modification
12.4(6)T	The **arp-ping** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	The **nopreservation** keyword was added.

Usage Guidelines

This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool.

The **nopreservation** keyword is used after the **prefix-length** or **netmask** keywords. It turns off the default behavior, which is known as IP address reservation. The **no** form of the command with the **nopreservation** keyword enables the default behavior, and reserves the first IP address in the NAT pool, making it unavailable for dynamic translation.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example shows that a route has been added to the NVI interface for the global address:

```
ip nat pool NAT 192.168.25.20 192.168.25.30 netmask 255.255.255.0 add-route
ip nat source list 1 pool NAT vrf group1 overload
```

Related Commands

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

ip nat service

To specify a port other than the default port, use the **ip nat service** command in global configuration mode. To disable the port, use the **no** form of this command.

ip nat service {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-number* | *access-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}

no ip nat service {**H225** | **allow-h323-even-rtp-ports** | **allow-h323-keepalive** | **allow-sip-even-rtp-ports** | **allow-skinny-even-rtp-ports** | **fullrange** {**tcp** | **udp**} **port** *port-number* | **list** {*access-list-number* | *access-list-name*} {**ESP spi-match** | **IKE preserve-port** | **ftp tcp port** *port-number*} | **alg** {**tcp** | **udp**} **dns** | **allow-multipart** | **mgcp** | **enable-mib** | **nbar** | **port-randomization** | **ras** | **rtsp** | **sip** {**tcp** | **udp**} **port** *port-number* | **skinny tcp port** *port-number*}

Syntax Description

H225	Specifies the H.323 to H.225 protocol.
allow-h323-even-rtp-ports	Specifies the even-numbered Real-time Transport Protocol (RTP) ports for the H.323 protocol.
allow-h323-keepalive	Specifies the H.323 keepalive.
allow-sip-even-rtp-ports	Specifies the even-numbered RTP ports for the Session Initiation Protocol (SIP).
allow-skinny-even-rtp-ports	Specifies the even-numbered RTP ports for the skinny protocol.
fullrange	Specifies all the available ports. The range is from 1 to 65535.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
port *port-number*	Specifies the port other than the default port in the range from 1 to 65533.
list *access-list-number*	Specifies the standard access list number in the range from 1 to 199.
access-list-name	Name of a standard IP access list.
ESP	Specifies the Security Parameter Index (SPI) matching IPsec pass-through.
spi-match	Specifies the SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE	Preserves the Internet Key Exchange (IKE) port, as required by some IPsec servers.
preserve-port	Preserves the UDP port in IKE packets.
ftp	Specifies FTP.
alg {**tcp** | **upd**} **dns**	Enables Domain Name System (DNS) processing with an Application-Level Gateway (ALG) for either TCP or UDP.
allow-multipart	Enables SIP multipart processing.
mgcp	Specifies the Media Gateway Control Protocol (MGCP).
enable-mib	Enables NAT MIB support.

nbar	Enables network-based application recognition (NBAR).
port-randomization	Specifies that ports are allocated randomly for Network Address Translation (NAT), instead of sequentially.
ras	Specifies the H.323-Registration, Admission, and Status (RAS) protocol.
rtsp	Specifies the Real Time Streaming Protocol (RTSP). This protocol is enabled by default on port 554 and requires NBAR.
sip	Specifies SIP. This protocol is enabled by default on port 5060.
skinny	Specifies the skinny protocol.

Command Default

DNS ALG processing is enabled for TCP and UDP.
H.323 even-numbered RTP port allocation is enabled.
Port randomization is disabled.
RTSP is enabled and requires NBAR.
Skinny even-numbered RTP port allocation is enabled.
UDP SIP even-numbered RTP port allocation is enabled.
UDP SIP is enabled on port 5060.
UDP SIP multipart processing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was modified. The **skinny** keyword was added.
12.2(8)T	This command was modified. The **sip** keyword was added.
12.2(15)T	This command was modified. The **ESP** and **spi-match** keywords were added to enable SPI matching on outside IPsec gateways. The **ike** and **preserve-port** keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	This command was modified. The **rtsp** and **mgcp** keywords were added.
12.3(11)T	This command was modified. The **allow-sip-even-rtp-ports** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was modified. The **nbar** keyword was added.
12.4(24)T	This command was modified. The **port-randomization** keyword was added.
15.0(1)M	This command was modified. The **alg**, **dns**, and **allow-multipart** keywords were added.
15.0(1)M2	This command was modified. The **enable-mib** keyword was added.
15.1(1)T2	This command was modified. The **tcp** keyword used along with the **sip** keyword was removed.

Release	Modification
15.0(1)M3	This command was modified. The **enable-mib** keyword was removed.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the Cisco CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service allow-h323-even-rtp-ports** command to force odd-numbered RTP port allocation for H.323.

Use the **no ip nat service allow-sip-even-rtp-ports** command to force odd-numbered RTP port allocation for SIP.

Use the **no ip nat service allow-skinny-even-rtp-ports** command to force odd-numbered RTP port allocation for the skinny protocol.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

By default SIP is enabled on port 5060; therefore NAT-enabled devices interpret all packets on this port as SIP call messages. If other applications in the system use port 5060 to send packets, the NAT service may corrupt the packet as it attempts to interpret the packet as a SIP call message.

A NAT-enabled Cisco device that is running Cisco IOS Release 12.3(7)T or a later release may experience an increase in CPU usage when upgrading from a previous release. RTSP and MGCP NAT ALG support was added in Cisco IOS Release 12.3(7)T, which requires NBAR. You can use the **no ip nat service nbar** command to disable NBAR processing, which can decrease the CPU utilization rate.

The **port-randomization** keyword can be used to prevent a security threat caused by the possibility of of predicting the next port number that NAT will allocate. This security threat is described in the Cisco Security Advisory titled *Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks*. Port randomization has the following limitations:

- It cannot be used with certain other NAT features, including port map, full-range, and Secure Network Address Translation (SNAT).
- It is supported only for the port in the Layer 4 header of the packet.

Use the **ip nat service allow-multipart** command to enable the processing of SIP multipart Session Description Protocol (SDP) packets.

NAT MIB support is turned off by default to avoid breakpoint exception crashes. To enable NAT MIB support, use the **enable-mib** keyword.

Examples

The following example shows how to configure the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the 20002 port of the Cisco CallManager:

```
ip nat service skinny tcp port 20002
```

The following example shows how to configure TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example shows how to configure SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service dns-reset-ttl

To reset the time-to-live (TTL) value for Domain Name System (DNS) resource records (RRs) going through Network Address Translation (NAT) to zero (0), use the **ip nat service dns-reset-ttl** command in global configuration mode. To prevent the TTL value for a DNS RR from being set to 0, use the **no** form of this command.

ip nat service dns-reset-ttl

no ip nat service dns-reset-ttl

Syntax Description

This command has no arguments or keywords.

Command Default

The TTL value is set to 0 for DNS RRs going through NAT.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

RFC 2694, *DNS extensions to Network Address Translators (DNS_ALG)*, states that the TTL value supplied in the original RRs for static address assignments is left unchanged. For dynamic address assignments, DNS_ALG will modify the TTL to be 0, so the RRs are used just for the transaction in progress, and not cached. RFC 2181, *Clarifications to the DNS Specification*, requires all RRs in an RRset (RRs with the same name, class, and type, but with different RDATA) to have the same TTL. So if the TTL of an RR is set to 0, all other RRs within the same RRset will also be adjusted by the DNS_ALG to be 0.

The **ip nat service dns-reset-ttl** command allows you to modify this behavior. The TTL values on all DNS RRs passing through NAT are set to 0 by default. This means that DNS servers or clients do not cache temporarily assigned RRs. Use the **no ip nat service dns-reset-ttl** command to disable the TTL value from being set to 0, and use the **ip nat service dns-reset-ttl** command to allow the TTL value to be reset to 0 again.

You may want to have a TTL value of 0 to prevent nonauthoritative servers from caching DNS RRs, perhaps in advance of changing a server's IP address. Allowing a nonzero value for DNS RRs enables remote name servers to cache the DNS RR information for a longer period of time, reducing the number of queries for the RR, while having the effect of lengthening the amount of time required to proliferate RR changes simultaneously.

Examples

The following example shows how to prevent DNS RRs that pass through NAT from having their TTL values set to 0:

```
Router(config)# no ip nat service dns-reset-ttl
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip dns primary	Configures router authority parameters for the DNS name server.
ip dns server	Enables the DNS server on the router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip dns primary	Displays the authoritative name server configuration for the router.
show ip nat statistics	Displays NAT statistics.
show ip nat translation	Displays active NAT translations.

ip nat service enable-sym-port

To enable the endpoint agnostic port allocation, use the **ip nat service enable-sym-port** command in global configuration mode. To disable the endpoint agnostic port allocation, use the **no** form of this command.

ip nat service enable-sym-port

no ip nat service enable-sym-port

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not issue this command, the *endpoint agnostic port allocation* is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use the **ip nat service enable-sym-port** command to enable the endpoint agnostic port allocation, which is also known as symmetric port allocation.

Note Use this command before you enable Network Address Translation (NAT). If you enable the symmetric port database after creating entries in the NAT database, then corresponding entries are not added to the symmetric port database.

Examples

In the following example, an access list is created and the inside source address is translated using NAT. The endpoint agnostic port allocation is enabled after the inside source address is translated.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# access list 1 permit 172.18.192.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface Ethernet 0/0
Router(config)# ip nat service enable-sym-port
Router(config)# end
```

Following are the list of entries which are made to the SymmetricPort (Sym Port) table, debugs, and Symmetric DB (Sym DB) when the command is issued and when the command is not entered:

```
NAT Symmetric Port Database: 1 entries
public ipaddr:port [tableid] | port# [refcount][syscount] | localaddr:localport [flags]
172.18.192.69:1024 [0] | 1025 [1] [0] | 172.18.192.69:1024 [0]
```

```
Sample SymPort Debugs:
If SymDB is not enabled or initiated:
NAT-SymDB: DB is either not enabled or not initiated.
If an entry needs to be inserted into SymDB:
NAT-SymDB: insert 172.18.192.69 1024 0
172.18.192.69 is the local address, 1024 is the local port, and 0 is the tableid
If SymDB lookup found an entry:
NAT-SymDB: [0] Entry was found for 172.18.192.69 -> 10.10.10.1: wanted 1024 got 1025
172.18.192.69 is the local address, 10.10.10.1 is the global address, 1024 is the
requested port, and 1025 is the allocated port
If entry was deleted from SymDB:
NAT-SymDB: deleting entry 172.18.192.69:1024
172.18.192.69 is the local address, 1024 is the local port.
```

Related Commands

Command	Description
show ip nat translations	Displays the list of translations entries.
show ip nat statistics	Displays the entries in the symmetric port database

ip nat sip-sbc

To configure a Cisco IOS hosted Network Address Translation (NAT) traversal for Session Border Controller (SBC), use the **ip nat sip-sbc** command in global configuration mode. To disable the Cisco IOS hosted NAT traversal for SBC, use the **no** form of this command.

ip nat sip-sbc proxy *inside-address inside-port outside-address outside-port* {**tcp | udp**} [**call-id-pool** *pool-name*] [**override** {**address** | **none** | **port**}] [**mode allow-flow-around**] [**mode allow-flow-through** *pool-name*] [**session-timeout** {*seconds* | **nat-default**}] [**registration-throttle inside-timeout** *seconds* **outside-timeout** *seconds*] [**vrf-list vrf-name** *vrf-name* | **no** | **exit**]

no ip nat sip-sbc proxy *inside-address inside-port outside-address outside-port* {**tcp | udp**} [**call-id-pool** *pool-name*] [**override** {**address** | **none** | **port**}] [**mode allow-flow-around**] [**mode allow-flow-through** *pool-name*] [**session-timeout** {*seconds* | **nat-default**}] [**registration-throttle inside-timeout** *seconds* **outside-timeout** *seconds*] [**vrf-list vrf-name** *vrf-name* | **no** | **exit**]

Syntax Description

proxy	Configures the address or port which the inside phones refer to, and configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port.
inside-address	Sets the Proxy's private IP address, which is configured on the inside phones.
inside-port	Sets the Proxy's private port.
outside-address	Sets the Proxy's public address, which is the actual proxy's address that NAT SBC changes the destination address to.
outside-port	Sets the Proxy's port.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
call-id-pool *pool-name*	(Optional) Specifies a dummy pool name from which the inside to outside SIP signaling packets' call ID is translated to a 1:1 maintained association rather than using the regular NAT pool.
override address	(Optional) Specifies the default override address mode.
override none	(Optional) Specifies that no override will be configured.
override port	(Optional) Specifies override port mode.
mode allow-flow-around	(Optional) Configures Real-Time Transport Protocol (RTP) for flow around for traffic between phones in the inside domain.
mode allow-flow-through *pool-name*	(Optional) Configures Real-Time Transport Protocol (RTP) for flow through for traffic between phones in the inside domain.
session-timeout *seconds*	(Optional) Configures the timeout duration for NAT entries pertaining to SIP signaling flows.
session-timeout nat-default	(Optional) Allows the default timeout to return to the NAT default timeout value of 5 minutes.
none	(Optional) Prevents modification of the out > in destination L3/L4 to the L3/L4 as saved in the sbc_appl_data of the door or NAT entry.
vrf-list vrf-name	(Optional) Defines SIP SBC VPN Routing and Forwarding (VRF) list names.

no	(Optional) Removes a name from the VRF list.
registration-throttle	(Optional) Defines the registration throttling parameter.
inside-timeout *seconds*	Timeout in seconds in the range of 1-536870**.**
outside-timeout *seconds*	Timeout in seconds in the range of 1-536870.
exit	(Required) Exit from SBC VRF configuration mode.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(15)T	The **allow-flow-through** and **registration-throttle** sub commands were added.

Usage Guidelines

The **proxy** keyword configures the address or port, which the inside phones refer to, and it configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port. This keyword installs an outside static port half-entry with OL as the inside address or port and OG as the outside address or port.

The **mode allow-flow-around** keyword enables the RTP to be flow around. This keyword is only applicable for traffic between phones in the inside domain.

The optional **vrf-list** keyword must be followed by a list of VRF names. After the outside static port entry is created, a static route is installed wit the destination IP address as OL and next hop as OG. The NAT entry created is associated with appropriate VRFs as configured by this command.

Examples

The following example shows how to configure a Cisco IOS hosted NAT traversal for SBC:

```
interface ethernet1/1
 ip nat inside
 ip forwarding A
!
interface ethernet1/2
 ip nat inside
 ip forwarding B
!
interface ethernet1/3
 ip nat outside
!
ip nat pool call-id-pool 1.1.1.1 1.1.1.100
ip nat pool outside-pool 2.2.2.1.1.1 2.2.2.1.1.10
ip nat pool inside-pool-A 169.1.1.1 169.1.1.10
ip nat pool inside-pool-B 170.1.1.1 170.1.1.10
ip nat inside source list 1 pool inside-pool-A vrf A overload
ip nat inside source list 2 pool inside-pool-B vrf B overload
ip nat outside list 3 pool outside-pool
ip nat inside source list 4 pool call-id-pool
```

```
!
access-list for VRF-A inside-phones
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 2 permit 172.1.1.0 0.0.0.255
!
access-=list for call-id-pool
access-list 4 permit 10.1.1.0 0.0.0.255
access-list 4 permit 20.1.1.0 0.0.0.255
!
ip nat sip-sbc
 proxy 200.1.1.1 5060 192.1.1.1 5060 protocol udp
 vrf-list
  vrf-name A
  vrf-name B
 call-id-pool call-id-pool
 session-timeout 300

 mode allow-flow-around
 override address
```

Related Commands

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

ip nat source

To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode.

Dynamic NAT

ip nat source {**list** {*access-list-number* | *access-list-name*} **interface** *type number* | **pool** *name*} [**overload** | **vrf** *name*]

no ip nat source {**list** {*access-list-number* | *access-list-name*} **interface** *type number* | **pool** *name*} **overload** | **vrf** *name*]

Static NAT

ip nat source {**static** {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*}} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

no ip nat source {**static** {**esp** *local-ip* **interface** *type number* | *local-ip global-ip*}} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Port Static NAT

ip nat source {**static** {**tcp** | **udp** {*local-ip local-port global-ip global-port* | **interface** *type number global-port*}} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

no ip nat source {**static** {**tcp** | **udp** {*local-ip local-port global-ip global-port* | **interface** *type number global-port*}} [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Network Static NAT

ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

no ip nat source static network *local-network global-network mask* [**extendable** | **no-alias** | **no-payload** | **vrf** *name*]

Syntax Description

list *access-list-number*	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access-list-name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
interface *type*	Specifies the interface type for the global address.
interface *number*	Specifies the interface number for the global address.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.

vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static *local-ip*	Sets up a single static translation. The *local-ip* argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from the RFC 1918, or obsolete.
local-port	Sets the local TCP/UDP port in a range from 1 to 65535.
static *global-ip*	Sets up a single static translation. The *local-ip* argument establishes the globally unique IP address of an inside host as it appears to the outside network.
global-port	Sets the global TCP/UDP port in the range from 1 to 65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits as alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
esp *local-ip*	Establishes IPSec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network *local-network*	Specified the local subnet translation.
global-network	Specifies the global subnet translation.
mask	Establishes the IP network mask to be used with subnet translations.

Command Modes

Global Configuration

Command History

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

Examples

The following example shows how to configure a virtual interface without inside or outside specification for the global address:

```
ip nat source list 1 pool NAT vrf bank overload
ip nat source list 1 pool NAT vrf park overload
ip nat source static 192.168.123.1 192.168.125.10 vrf services
```

Related Commands

Command	Description
ip nat enable	Configures an interface connecting VPNs and the Internet for NAT translation.
ip nat pool	Defines a pool of IP addresses for Network Address Translation.

ip nat stateful id

To designate the members of a translation group, use the **ip nat stateful id** command in global configuration mode. To disable the members of a translation group or reset default values, use the **no** form of this command.

ip nat stateful id *id-number* {**redundancy** *name* **mapping-id** *map-number* [**protocol** {**tcp** | **udp**}] [**as-queuing** {**disable** | **enable**}] | {**primary** *ip-address-primary* **backup** *ip-address-backup* **peer** *ip-address-peer* **mapping-id** *mapping-id-number*}

no ip nat stateful id *id-number*

Syntax Description

id-number	Unique number given to each router in the stateful translation group.
redundancy *name*	Establishes Hot Standby Routing Protocol (HSRP) as the method of redundancy.
mapping-id *map-number*	Specifies whether or not the local Stateful (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
protocol	(Optional) Enables the HSRP UDP default to be changed to TCP.
tcp	(Optional) Establishes the Transmission Control Protocol.
udp	(Optional) Establishes the User Datagram Protocol.
as-queuing disable	(Optional) Disables the use of queuing with asymmetric routing in HSRP mode.
as-queuing enable	(Optional) Enables the use of queuing with asymmetric routing in HSRP mode.
primary i*p-address-primary*	Manually establishes redundancy for the primary router.
backup i*p-address-backup*	Manually establishes redundancy for the backup router.
peer *ip-address-peer*	Specifies the IP address of the peer router in the translation group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(3)	The **protocol** and **as-queuing** keywords were added.
12.4(4)T	This command was intregrated into Cisco IOS Release 12.4(4)T.
15.0(1)M2	The **as-queuing** keyword was removed.

Usage Guidelines

This command has two forms: HSRP stateful NAT and manual stateful NAT. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

In HSRP mode, the default TCP can be changed to UDP by using the optional **protocol udp** keywords with the **redundancy keyword**.

To disable the queuing during asymmetric routing in HSRP mode, use the optional **as-queuing disable** keywords with the **redundancy** keyword.

Examples

The following example shows how to configure SNAT with HSRP:

```
!
standby delay minimum 30 reload 60
standby 1 ip 10.1.1.1
standby 1 name SNATHSRP
standby 1 preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
as-queuing disable
protocol udp
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

The following example shows how to manually configure SNAT:

```
ip nat stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10

ip nat stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

Related Commands

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

ip nat translation

The **ip nat translation** command is replaced by the **ip nat translation** (timeout) and **ip nat translation max-entries** commands. See these commands for more information.

ip nat translation (timeout)

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** *port-number* | **udp** *port-number*} | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**} {*seconds* | never}

no ip nat translation {**arp-ping-timeout** | **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **port-timeout** {**tcp** *port-number* | **udp** *port-number*} | **pptp-timeout** | **routemap-entry-timeout** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout**}

Syntax Description

arp-ping-timeout	Specifies that the timeout value applies to the Address Resolution Protocol (ARP) ping.
dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. The default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
tcp	Specifies Transport Control Protocol (TCP).
udp	Specifies User Datagram Protocol (UDP).
port-number	Port number. The range is from 1 to 65535.
pptp-timeout	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86,400 seconds (24 hours).
routemap-entry-timeout	Specifies that the timeout applies for routemap created half entry.
syn-timeout	Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
timeout	Specifies that the timeout value applies to dynamic translations except for overload translations. The default is 86,400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. The default is 300 seconds (5 minutes).
seconds	Number of seconds after which the specified port translation times out.
never	Specifies no port translation time out.

Defaults

timeout: 86,400 seconds (24 hours)
udp-timeout: 300 seconds (5 minutes)
dns-timeout: 60 seconds (1 minute)
tcp-timeout: 86,400 seconds (24 hours)

finrst-timeout: 60 seconds (1 minute)
icmp-timeout: 60 seconds (1 minute)
pptp-timeout: 86,400 seconds (24 hours)
syn-timeout: 60 seconds (1 minute)

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	This command was modified. The **arp-ping-timeout** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **routemap-entry-timeout**, **tcp**, **udp**, and *port-number* keywords and arguments were added.

Usage Guidelines

When port translation is configured, each entry contains more context about the traffic that is using it, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an rapid spanning-tree (RST) or FIN bit is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example shows how to configure the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
Router# configure terminal
Router(config)# ip nat translation udp-timeout 600
```

Related Commands

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

ip nat translation max-entries

To limit the size of a Network Address Translation (NAT) table to a specified maximum, use the **ip nat translation max-entries** command in global configuration mode. To remove a specified limit, use the **no** form of this command.

ip nat translation max-entries [**all-host** | **all-vrf** | **host** *ip-address* | **list** {*listname* | *listnumber*} | **vrf** *name*] *number*

no ip nat translation max-entries [**all-host** | **all-vrf** | **host** *ip-address* | **list** {*listname* | *listnumber*} | **vrf** *name*] *number*

Syntax Description

all-host	(Optional) Constrains each host by the specified number of NAT entries.
all-vrf	(Optional) Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
host	(Optional) Constrains an IP address by the specified NAT limit.
ip-address	(Optional) IP address subject to the NAT limit.
list	(Optional) Constrains an access control list (ACL) by the specified NAT limit.
listname	ACL name subject to the NAT limit.
listnumber	ACL number subject to the NAT limit.
vrf	(Optional) Constrains an individual VRF instance by the specified NAT limit.
name	(Optional) Name of the VRF instance subject to the NAT limit.
number	Maximum number of allowed NAT entries. Range is from 1 to 2147483647.

Command Default

No maximum size is specified for the NAT table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **vrf** *name* keyword and argument pair was removed from Cisco 7600 series routers.

Usage Guidelines

Before you configure a NAT rate limit, you must first classify the current NAT usage and determine the sources of requests for NAT translations. If a specific host, an access control list, or a VRF instance is generating an unexpectedly high number of NAT requests, it may be the source of a virus or worm attack.

Once you have identified the source of excess NAT requests, you can set a NAT rate limit that constrains a specific host, access control list, or VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.

Note When using the **no** form of the **ip nat translation max-entries** command, you must specify the type of NAT rate limit you want to remove and its current value. For more information about how to display the current NAT rate limit settings, see the **show ip nat statistics** command.

Examples

The following examples show how to configure the rate-limiting NAT translation.

Setting a General NAT Limit

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
ip nat translation max-entries 300
```

Setting NAT Limits for VRF Instances

The following example shows how to limit each VRF instance to 200 NAT entries:

```
ip nat translation max-entries all-vrf 200
```

The following example shows how to limit the VRF instance named vrf1 to 150 NAT entries:

```
ip nat translation max-entries vrf vrf1 150
```

The following example shows how to limit the VRF instance named vrf2 to 225 NAT entries, but limit all other VRF instances to 100 NAT entries each:

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

Setting NAT Limits for Access Control Lists

The following example shows how to limit the access control list named vrf3 to 100 NAT entries:

```
ip nat translation max-entries list vrf3 100
```

Setting NAT Limits for an IP Address

The following example shows how to limit the host at IP address 10.0.0.1 to 300 NAT entries:

```
ip nat translation max-entries host 10.0.0.1 300
```

Related Commands

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

Command	Description
ip nat translation (timeout)	Changes the NAT timeout value.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

name

To configure the redundancy group with a name, use the **name** command in redundancy application group configuration mode**.** To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

Syntax Description

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

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 name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

nat64 enable

To enable stateless Network Address Translation 64 (NAT64) on an interface, use the **nat64 enable** command in interface configuration mode. To disable the NAT64 configuration on an interface, use the **no** form of this command.

nat64 enable

no nat64 enable

Syntax Description

This command has no arguments or keywords.

Command Default

NAT64 is not enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example shows how to enable stateless NAT64 on a Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# nat64 enable
Router(config-if)# end
```

Related Commands

Command	Description
show nat64 adjacency	Displays information about the NAT64-managed adjacencies.
show nat64 ha status	Displays information about the NAT64 HA status.
show nat64 statistics	Displays statistics about a NAT64 interface and the transmitted and dropped packet count.

nat64 prefix

To assign a global or interface-specific Network Address Translation 64 (NAT64) stateless prefix, use the **nat64 prefix** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

nat64 prefix stateless *ipv6-prefix*/*prefix-length*

no nat64 prefix stateless

Syntax Description

stateless	Specifies the stateless prefix.
ipv6-prefix	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*	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.

Command Default

No NAT64 translation is performed.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

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

Usage Guidelines

The **nat64 prefix stateless** command uses a prefix and prefix length for IPv4-translatable IPv6 addresses. Use the **nat64 prefix stateless** command in global configuration mode to assign a global NAT64 stateless prefix or in interface configuration mode to assign an unique NAT64 stateless prefix for each interface. In interface configuration mode, a stateless prefix should be configured on an IPv6-facing interface.

All packets coming to an IPv6 interface are matched against the configured prefix, and the matched packets are translated to IPv4. Similarly, the packets that the IPv6 interface sends use the stateless prefix to construct the source and destination IPv6 address.

Note A maximum of one global stateless prefix and one stateless prefix per interface is supported.

If NAT64 is enabled on an interface that does not have a stateless prefix configured, then the global stateless prefix is used. However, if a global prefix and an interface prefix are configured, then the interface prefix is used for stateless NAT64 translation. The use of a stateless prefix on an interface has priority over the configured global stateless prefix.

Examples

The following example shows how to configure a global NAT64 stateless prefix:

```
Router# configure terminal
Router(config)# nat64 prefix stateless 2001::7001:10A/96
Router(config)# end
```

The following example shows how to assign a NAT64 stateless prefix for a Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# nat64 prefix stateless 2001:0DB8:0:1::/96
Router(config-if# end
```

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.
show nat64 prefix stateless	Displays information about the configured NAT64 stateless prefixes.

nat64 route

To specify the Network Address Translation 64 (NAT64) stateless prefix to which an IPv4 prefix should be translated, use the **nat64 route** command in global configuration mode. To disable the configuration, use the **no** form of this command.

nat64 route *ipv4-prefix/mask interface-type interface-number*

no nat64 route *ipv4-prefix/mask*

Syntax Description

ipv4-prefix/mask	Length of the IPv4 prefix and the mask.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-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

No NAT64 routing is performed.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

A prefix that is configured on an interface is used as the stateless prefix on that interface. If no interface-specific prefix is configured, the configured global prefix is used for NAT64 translation.

Examples

The following example shows how to assign an IPv4 prefix and mask to an interface:

```
Router# configure terminal
Router(config)# nat64 route 192.168.0.0/24 gigabitethernet0/0/1
Router(config)# exit
```

Related Commands

Command	Description
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
show nat64 routes	Displays information about the configured NAT64 routes.

preempt

To enable preemption on the redundancy group, use the **preempt** command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

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

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Examples

The following example shows how to enable preemption on the redundancy group:

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

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

priority

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]

no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

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

The priority of the redundancy group is used to determine a redundancy group’s active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

protocol

To define a protocol instance in a redundancy group, use the **protocol** command in redundancy application group configuration mode**.** To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*

no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

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

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

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

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

redundancy application reload group

To manually force a state switchover for the redundancy group, use the **redundancy application reload group** command in user EXEC or privileged EXEC mode**.** To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy application reload group *id* [**peer** | **self**]

Syntax Description

id	Redundancy group ID.
peer	Force the peer in the redundancy group to reload.
self	Force this member of the redundancy group to reload.

Command Default

Forces this member of the redundancy group to reload.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

You can use this command to reload the peer only on the active member of the redundancy group to reload the standby member of the redundancy group.

Examples

The following example shows how to reload the standby peer in a redundancy group:

```
Router# redundancy application reload group 2 peer
```

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.

redundancy group

To configure the virtual IP address for the redundancy group, use the **redundancy group** command in interface configuration mode. To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

no redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

Syntax Description

id	Redundancy group ID.
ip *address*	Specifies the IP address of the interface.
exclusive	Specifies whether the interface is not shared with another redundancy group.
decrement *value*	(Optional) Amount decremented from the priority when the L1 state of the interface goes down. This overrides the default amount for the redundancy group. The range is from 1 to 255.

Command Default

Virtual IP address is not configured.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The virtual IP address and the physical address must in the same subnet.

Examples

The following example shows how to configure the redundancy group redundancy traffic interface:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy group 2 ip 1.2.3.4 exclusive
```

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.
data	Configures the data interface type and number for a redundancy group.

Command	Description
group	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.
redundancy rii	Configures the RII for the redundancy group.

redundancy rii

To configure the redundancy interface identifier (RII) for the redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode**.** To remove the control interface from the redundancy group, use the **no** form of this command.

redundancy rii *id*

no redundancy rii *id*

Syntax Description

id	Redundancy interface identifier. The range is from 1 to 65535.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Every interface associated with one or more Redundancy Groups must have a unique RII assigned to it. RII allows interfaces to have a one-to-one mapping between peers.

Examples

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

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

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.
data	Configures the data interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
redundancy group	Configures the virtual IP address for a redundancy group.

show ip nat nvi statistics

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

show ip nat nvi statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show ip nat nvi statistics

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

Table 31 describes the fields shown in the display.

Table 31 show ip nat nvi statistics Field Descriptions

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

Related Commands

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

show ip nat nvi translations

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show ip nat nvi translations

Pro    Source global       Source local        Destin  local       Destin  global
icmp   172.20.0.254:25    172.20.0.130:25     172.20.1.1:25       10.199.199.100:25
icmp   172.20.0.254:26    172.20.0.130:26     172.20.1.1:26       10.199.199.100:26
icmp   172.20.0.254:27    172.20.0.130:27     172.20.1.1:27       10.199.199.100:27
icmp   172.20.0.254:28    172.20.0.130:28     172.20.1.1:28       10.199.199.100:28
```

Table 32 describes the fields shown in the display.

Table 32 show ip nat nvi translations Field Descriptions

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

Table 32 show ip nat nvi translations Field Descriptions (continued)

Field	Description
Destin local	Destination local address.
Destin global	Destination global address.

Related Commands

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

show ip nat statistics

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

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

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

```
Router# show ip nat statistics

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

Table 33 describes the significant fields shown in the display.

Table 33 show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.

Table 33 show ip nat statistics Field Descriptions (continued)

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

Related Commands

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

show ip nat translations

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The **vrf** *vrf-name* keyword and argument combination was added.
12.2(15)T	The **esp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.4.2	The **inside** and **outside** keywords were added.

Examples

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

```
Router# show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
--- 10.69.233.209     192.168.1.95       ---                ---
--- 10.69.233.210     192.168.1.89       ---                --
```

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

```
Router# show ip nat translations

Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
```

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

```
Router# show ip nat translations verbose

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

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

```
Router# show ip nat translations vrf abc

Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.1            192.168.121.113    ---                ---
--- 10.2.2.2            192.168.122.49     ---                ---
--- 10.2.2.11           192.168.11.1       ---                ---
--- 10.2.2.12           192.168.11.3       ---                ---
--- 10.2.2.13           172.16.5.20        ---                ---

Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.3            192.168.121.113    ---                ---
--- 10.2.2.4            192.168.22.49      ---                ---
```

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

```
Router# show ip nat translations esp

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0       192.168.122.20:0      192.168.22.20:0
192.168.22.20:28726CD9
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
```

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

```
Router# show ip nat translation esp verbose

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

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

```
Router# show ip nat translations inside 10.69.233.209
```

```
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip nat translations Field Descriptions

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

Related Commands

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

show ip snat

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

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

Syntax Description

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

Command Modes

EXEC

Command History

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

Examples

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

```
Router# show ip snat distributed

Stateful NAT Connected Peers

SNAT: Mode PRIMARY
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
```

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

```
Router# show ip snat distributed verbose

SNAT: Mode PRIMARY
Stateful NAT Connected Peers

:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
:InMsgs 7, OutMsgs 7, tcb 0x63EBA408, listener 0x0
```

show nat64 adjacency

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show nat64 adjacency all

Adjacency Counts
 IPv4 Adjacencies: 2
 IPv6 Adjacencies: 1
 Stateless Prefix Adjacency Ref Count: 1

Adjacencies
 IPv6 Adjacencies
    ::42
 IPv4 Adjacencies
    0.0.19.137 (5001)
    0.0.19.140 (5004)
```

Table 35 describes the significant fields shown in the display.

Table 35 show nat64 adjacency all Field Descriptions

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

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 ha status

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

show nat64 ha status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show nat64 ha status

NAT64 HA Status

 Role: active
 Peer is ready: TRUE
 Peer is compatible: TRUE
 Synchronization enabled: TRUE
 Is hot (standby): FALSE
 Bulk sync PID: NO_PROCESS
 ISSU negotiation status: IPC, CF
 ISSU context IDs: IPC(198), CF(197)
 Synchronization capabilities: 0x00000001
  Adjacency mappings: TRUE
 CF info: handle(0x0000011B), peer ready(TRUE),
  flow control(TRUE)(FALSE)(0x0)
 Initialized: HA(TRUE) ISSU(TRUE)

 Message stats:
  Adjacency mapping: rx(0) tx(5001) tx err(0)
  Bulk sync done: rx(0) tx(1) tx err(0)
 Errors:
  Bulk sync: 0
  CF tx: 0
```

Table 36 describes the significant fields shown in the display.

Table 36 show nat64 ha status Field Descriptions

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

Related Commands

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

show nat64 prefix stateless

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

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

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show nat64 prefix stateless global

Global Prefix: is valid, 2001::/96

IFs Using Global Prefix

   Fa0/3/4
   Fa0/3/5
```

Table 37 describes the significant fields shown in the display.

Table 37 show nat64 prefix stateless global Field Descriptions

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

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

```
Router# show nat64 prefix stateless interfaces

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

Table 36 describes the significant fields shown in the display.

Table 38 show nat64 prefix stateless interfaces Field Descriptions

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

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

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

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

Related Commands

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

show nat64 routes

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

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

Syntax Description

adjacency	(Optional) Displays the route for an adjacency address.
address	(Optional) Adjacency address for lookup.
interface	(Optional) Displays routes pointing to an interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional) Displays the route of an IPv4 prefix.
prefix-length	(Optional) Length of the IPv4 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show nat64 routes

IPv4 Prefix          Adj. Address    Enabled   Output IF    Global    IPv6 Prefix
192.0.2.1/24         0.0.19.137      FALSE     Fa0/3/4
198.51.100.253/24    0.0.19.140      TRUE      Fa0/3/0      FALSE     3001::/96
```

Table 36 describes the significant fields shown in the display.

Table 39 show nat64 routes Field Descriptions

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

Related Commands

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

show nat64 statistics

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

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

Syntax Description

global	(Optional) Displays global NAT64 statistics.
interface	(Optional) Displays statistics for an interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional) Displays statistics for a specified prefix.
ipv6-prefix	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. The valid values are from 0 to 128.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show nat64 statistics

NAT64 Statistics

Global Stats:
   Packets translated (IPv4 -> IPv6): 21
   Packets translated (IPv6 -> IPv4): 15

GigabitEthernet0/0/1 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 5
   Packets translated (IPv6 -> IPv4): 0
   Packets dropped: 0
GigabitEthernet1/2/0 (IPv4 configured, IPv6 configured):
   Packets translated (IPv4 -> IPv6): 0
   Packets translated (IPv6 -> IPv4): 5
   Packets dropped: 0
```

Table 40 describes the significant fields shown in the display.

Table 40 show nat64 statistics Field Descriptions

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

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show platform hardware qfp feature

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

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

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
alg	Displays the Application Level Gateway (ALG) information of the processor.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.
protocol	One of the following protocols: • dns • exec • ftp • h323 • http • ldap • login • netbios • rtsp • shell • sip • skinny • smtp • tftp
clear	Clears the ALG counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the Network Basic Input Output System (NetBIOS) protocol and the following keywords were added: **netbios-dgm**, **netbios-ns**, and **netbios-ssn**.

Usage Guidelines

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

Examples

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

```
Router# show platform hardware qfp active feature alg statistics netbios

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

Table 41 describes the significant fields shown in the display.

Table 41 show platform hardware qfp feature Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Counter tracking number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Counters tracking number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Counter tracking number of direct unique NetBIOS packets processed.
Direct group packets	Counter tracking number of direct group NetBIOS packets processed.

Table 41 show platform hardware qfp feature Field Descriptions (continued)

Field	Description
Broadcast packets	Counter tracking number of BROADCAST NetBIOS packets processed.
DGM Error packets	Counter tracking number of Datagram Error NetBIOS packets processed.
Query request packets	Counter tracking number of query request NetBIOS packets processed.
Positive Qry response packets	Counter tracking number of positive query response NetBIOS packets processed.
Negative Qry response packets	Counter tracking number of negative query response NetBIOS packets processed.
Unknown packets	Counter tracking number of unknown packets.
Total error packets	Counter tracking number of error packets.

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs features in QFP.

show platform software trace message

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

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

Syntax Description

process	The process in which the tracing level is being set. The following keywords are available: • **chassis-manager**—The Chassis Manager process. • **cpp-control-process**—The Cisco packet processor (CPP) Control process. • **cpp-driver**—The CPP driver process. • **cpp-ha-server**—The CPP high availability (HA) server process. • **cpp-service-process**—The CPP service process. • **forwarding-manager**—The Forwarding Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **ios**—The Cisco IOS process. • **logger**—The logging manager process. • **pluggable-services**—The pluggable services process. • **shell-manager**—The Shell Manager process.
hardware-module	Tthe hardware module where the process whose trace level is being set is running. The following keywords are available: • **carrier-card**—The process is on an SPA Interface Processor (SIP). • **forwarding-processor**—The process is on an embedded services processor (ESP). • **route-processor**—The process is on an route processor (RP).
slot	The slot of the hardware module. Options are as follows: • *number*—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter **2**. • *SIP-slot*/*SPA-bay*—The number of the SIP router slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter **3/2**. • **cpp active**—The CPP in the active ESP. • **cpp standby**—The CPP in the standby ESP. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **fp active**—The active ESP. • **fp standby**—The standby ESP.

- **r0**—The RP in RP slot 0.
- **r1**—The RP in RP slot 1.
- **rp active**—The active RP.
- **rp standby**—The standby RP.
- **qfp active**—The active Quantum Flow Processor (QFP)

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

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

Related Commands

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

show redundancy application group

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2


Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED


RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.


Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED


RG Protocol RG 2
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Standby Peer: Not Present.
```

Table 42 describes the significant fields shown in the display.

Table 42 show redundancy application group all Field Descriptions

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

Related Commands

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

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

show redundancy application transport

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

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

Syntax Description

client	Displays transport client specific information.
group-id	(Optional) Redundancy group group is. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application transport group 1

Transport Information for RG (1)
```

Related Commands

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

show redundancy application control-interface

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application control-interface group 2

The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

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

show redundancy application faults

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application faults group 2

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

Table 43 describes the significant fields shown in the display.

Table 43 show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group. This field is important when monitoring redundancy group switchover and when configuring interface tracking.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.

Related Commands

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

show redundancy application protocol

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application protocol 3

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

Table 44 describes the significant fields shown in the display.

Table 44 show redundancy application protocol Field Descriptions

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

Related Commands

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

show redundancy application if-mgr

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

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

Syntax Description

group	(Optional) Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. The range is from 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application if-mgr group 2

RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 =========================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

Table 45 describes the significant fields shown in the display.

Table 45 show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.

Table 45 show redundancy application if-mgr Field Descriptions (continued)

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

Related Commands

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

show redundancy application data-interface

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show redundancy application data-interface group 1

The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

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

shutdown

To shut down a group manually, use the **shutdown** command in redundancy application group configuration mode**.** To enable a redundancy group, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The group is active.

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

When a group is shutdown, it does not participate in the role negotiation. The group remains in the shutdown state until you execute the **no shutdown** command.

Examples

The following example shows how to shut down a group named group1:

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

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

timers hellotime

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

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

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

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages. The range is from 250 to 1000.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages. The range is from 750 to 3000.
seconds	Specifiesthe interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	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.

NHRP Commands

clear ip nhrp

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was modified. Support was added for the **shortcut** keyword.

Usage Guidelines

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

Examples

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

```
Router> clear ip nhrp
```

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

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

Related Commands

Command	Description
show ip nhrp	Displays the NHRP cache.

ip nhrp authentication

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

ip nhrp authentication *string*

no ip nhrp authentication [*string*]

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

All routers configured with NHRP within one logical nonbroadcast multiaccess (NBMA) network must share the same authentication string.

Examples

In the following example, the authentication string named specialxx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication specialxx
```

ip nhrp group

To configure a Next Hop Resolution Protocol (NHRP) group on a spoke, use the **ip nhrp group** command in interface configuration mode. To remove an NHRP group, use the **no** form of this command.

ip nhrp group *group-name*

no ip nhrp group *group-name*

Syntax Description

group-name	Specifies an NHRP group name.

Command Default

No NHRP groups are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

After you create an NHRP group on a spoke, you use the **ip nhrp map group** command to map the group to a QoS policy map.

Examples

The following example shows how to create two NHRP groups named small and large.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp group small
Router(config-if)# ip nhrp group large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

ip nhrp holdtime

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

ip nhrp holdtime *seconds*

no ip nhrp holdtime [*seconds*]

Syntax Description

seconds	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses.

Defaults

7200 seconds (2 hours)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
ip nhrp holdtime 3600
```

ip nhrp interest

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ip nhrp interest** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip nhrp interest *access-list-number*

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

Syntax Description

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

Defaults

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command with the **access-list** command to control which IP packets trigger NHRP requests.

The **ip nhrp interest** command controls which packets cause NHRP address resolution to take place; the **ip nhrp use** command controls how readily the system attempts such address resolution.

Examples

In the following example, any TCP traffic can cause NHRP requests to be sent, but no other IP packets will cause NHRP requests:

```
ip nhrp interest 101
access-list 101 permit tcp any any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp map

To statically configure the IP-to-nonbroadcast multiaccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ip nhrp map *ip-address nbma-address*

no ip nhrp map *ip-address nbma-address*

Syntax Description

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

Defaults

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured to be 192.0.0.1 and the NBMA address for 10.0.1.3 is 192.2.7.8.

```
interface tunnel 0
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.1.3
 ip nhrp map 10.0.0.1 192.0.0.1
 ip nhrp map 10.0.1.3 192.2.7.8
```

Related Commands\

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

ip nhrp map group

To associate a Next Hop Resolution Protocol (NHRP) group to a QoS policy map, use the **ip nhrp map group** command in interface configuration mode. To remove an association, use the **no** form of this command.

ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

no ip nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

Syntax Description

group-name	Specifies an NHRP group name.
qos-policy-map-name	Specifies a QoS policy map name.

Command Default

No mappings are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

The command allows a QoS policy in the output direction only.

Examples

The following example shows how to map two NHRP groups named small and large to two QoS policy maps named qos-small and qos-large respectively.

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel 0
Router(config-if)# ip nhrp map group small service-policy output qos-small
Router(config-if)# ip nhrp map group large service-policy output qos-large
```

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

ip nhrp map multicast

To configure nonbroadcast multiaccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** command in interface configuration mode. To remove the destinations, use the **no** form of this command.

ip nhrp map multicast *nbma-address*

no ip nhrp map multicast *nbma-address*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command applies only to tunnel interfaces.

The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2. Addresses 10.0.0.1 and 10.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.

```
interface tunnel 0
 ip address 10.0.0.3 255.0.0.0
 ip nhrp map multicast 10.0.0.1
 ip nhrp map multicast 10.0.0.2
```

ip nhrp map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings, use the **ip nhrp map multicast dynamic** command in interface configuration mode. To disable this functionality or to clear dynamic entries, use the **no** form of this command.

ip nhrp map multicast dynamic

no ip nhrp map multicast dynamic

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M3	This command was modified to enable the clearing of all dynamic entries in the multicast table by using the **no** form of this command.

Usage Guidelines

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

You can clear all dynamic entries in the multicast table by using the **no** form of this command.

Examples

The following example shows how to enable the **ip nhrp map multicast dynamic** command on the hub router:

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwith 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 10.17.0.1 255.255.255.0
```

ip nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ip nhrp max-send** interface configuration command. To restore this frequency to the default value, use the **no** form of this command.

ip nhrp max-send *pkt-count* **every** *seconds*

no ip nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
every *seconds*	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults

pkt-count: 100 packets
seconds: 10 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *seconds* argument.

- This command needs to take into consideratin the number of spoke routers being handled by this hub and how often they send NHRP registration requests. To support this load you would need:

  Number of spokes / registration timeout * *Max-send-interval*

  – Example

  500 spokes with 100 second Registration timeout

  Max send value = 500/100*10 = 50

- The Maximum number of spoke-spoke tunnels that are expected to be up at any one time across the whole DMVPN network.

  spoke-spoke tunnels/NHRP holdtime * Max-send-interval

  This would cover spoke-spoke tunnel creation and the refreshing of spoke-spoke tunnels that are used for longer periods of time.

- Example

  2000 spoke-spoke tunnels with 250 second hold timeout

  Max send value = 2000/250*10 = 80

  Then add these together and multiply this by 1.5 - 2.0 to give a buffer.

- Example

  Max send = (50 + 80) * 2 = 260

- The max-send-interval can be used to keep the long term average number of NHRP messages allowed to be sent constant, but allow greater peaks.

  - Example

    400 messages in 10 seconds

  In this case it could peak at approximately 200 messages in the first second of the 10 second interval, but still keep to a 40 messages per second average over the 10 second interval.

    4000 messages in 100 seconds

  In this case it could peak at approximately 2000 messages in the first second of the 100 second interval, but it would still be held to 40 messages per second average over the 100 second interval. In the second case it could handle a higher peak rate, but risk a longer period of time when no messages can be sent if it used up its quota for the interval.

By default, the maximum rate at which the software sends NHRP packets is five packets per 10 seconds. The software maintains a per-interface quota of NHRP packets (whether generated locally or forwarded) that can be sent.

Examples

In the following example, only one NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ip nhrp max-send 1 every 60
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp network-id

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

ip nhrp network-id *number*

no ip nhrp network-id [*number*]

Syntax Description

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

Defaults

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables NHRP on the interface:

```
ip nhrp network-id 1
```

ip nhrp nhs

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

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases

ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Cisco IOS Release 15.1(2)T and Later Releases

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

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

Syntax Description

nhs-address	Address of the next-hop server being specified.
net-address	(Optional) IP address of a network served by the next-hop server.
netmask	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.
max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Defaults

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The *net-address* and *mask* arguments were removed and the **nbma**, *nbma-address*, *FQDN-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.

Usage Guidelines

Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address* argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

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

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

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

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

ip nhrp record

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

ip nhrp record

no ip nhrp record

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ip nhrp responder** command.

Examples

The following example suppresses forward record and reverse record options:

```
no ip nhrp record
```

Related Commands

Command	Description
ip nhrp responder	Designates the primary IP address of which interface the Next Hop Server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

ip nhrp redirect

To enable Next Hop Resolution Protocol (NHRP) redirect, use the **ip nhrp redirect** command in interface configuration mode. To remove the NHRP redirect, use the **no** form of this command.

ip nhrp redirect [**timeout** *seconds*]

no ip nhrp redirect [**timeout** *seconds*]

Syntax Description

timeout *seconds*	Indicates the interval, in seconds, that the NHRP redirects are sent for the same nonbroadcast multiaccess (NBMA) source and destination combination. The range is from 2 to 30 seconds.

Command Default

NHRP redirect is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NHRP redirect message is an indication that the current path to the destination is not optimal. The receiver of the message should find a better path to the destination.

This command generates an NHRP redirect traffic indication message if the incoming and outgoing interface is part of the same DMVPN network. The NHRP shortcut switching feature depends on receiving the NHRP redirect message. NHRP shortcut switching does not trigger an NHRP resolution request on its own. It triggers an NHRP resolution request only after receiving an NHRP redirect message.

Most of the traffic would follow a spoke-hub-spoke path. NHRP redirect is generally required to be configured on all the DMVPN nodes in the event the traffic follows a spoke-spoke-hub-spoke path, which is unlikely the case.

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to enable NHRP redirects on the interface:

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel0
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp shortcut	Enables NHRP shortcut switching.

ip nhrp registration

To enable the client to not set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp registration** command in interface configuration mode. To reenable this functionality, use the **no** form of this command.

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

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

Syntax Description

timeout *seconds*	(Optional) Time between periodic registration messages. • *seconds*—Number of seconds. The range is from 1 through the value of the NHRP hold timer. • If the **timeout** keyword is not specified, NHRP registration messages are sent every number of seconds equal to 1/3 the value of the NHRP hold timer.
no-unique	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.

Defaults

This command is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced.
12.3(7.2)	The **timeout** keyword and *seconds* argument were added. In addition, effective with Cisco IOS Release 12.3(7.2), this command replaced the **ip nhrp registration no-unique** command.
12.3(7)T	The **timeout** keyword and *seconds* argument were integrated into Cisco IOS Release 12.3(7)T. In addition, the replacement of the **ip nhrp registration no-unique** command with this command was integrated into Cisco IOS Release 12.3(7)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If the unique flag is set in the NHRP registration request packet, a next-hop server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address, for example via DHCP, and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration command and no-unique** keyword, the unique flag is not set, and the NHS can override the old registration information.

This command and keyword combination is useful in an environment where client IP addresses can change frequently such as a dial environment.

Examples

The following example configures the client to not set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration no-unique
```

The following example shows that the registration timeout is set to 120 seconds, and the delay is set to 5 seconds:

```
interface FastEthernet 0/0
 ip nhrp registration 120
```

Related Commands

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

ip nhrp registration no-unique

The **ip nhrp registration no-unique** command is replaced by the **ip nhrp registration command.** See the **ip nhrp registration** command for more information.

ip nhrp responder

To designate the primary IP address the Next Hop Server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** command in interface configuration mode. To remove the designation, use the **no** form of this command.

ip nhrp responder *interface-type interface-number*

no ip nhrp responder [*interface-type*] [*interface-number*]

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

If an NHRP requestor wants to know which next-hop server generates an NHRP reply packet, it can request that information through the Responder Address option. The next-hop server that generates the NHRP reply packet then complies by inserting its own IP address in the Responder Address option of the NHRP reply. The next-hop server uses the primary IP address of the specified interface.

If an NHRP reply packet being forwarded by a next-hop server contains the IP address of that next-hop server, the next-hop server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a next-hop server to supply the primary IP address of serial interface 0 in the NHRP reply packet:

```
ip nhrp responder serial 0
```

ip nhrp server-only

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

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

no ip nhrp server-only

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).

Examples

The following example configures the interface to operate in server-only mode:

```
ip nhrp server-only
```

ip nhrp shortcut

To enable Next Hop Resolution Protocol (NHRP) shortcut switching, use the **ip nhrp shortcut** command in interface configuration mode. To remove shortcut switching from NHRP, use the **no** form of this command.

ip nhrp shortcut

no ip nhrp shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

The NHRP shortcut switching is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration the spokes are populated with a full routing table with next-hop being the other spokes.

Examples

The following example shows how to configure an NHRP shortcut on an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface Tunnel0
Router(config-if)# ip address 192.2.0.11 255.255.255.0
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp map multicast 192.2.0.2
Router(config-if)# ip nhrp map 192.2.0.2 192.2.0.13
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 192.2.0.11
Router(config-if)# ip nhrp shortcut
Router(config-if)# ip nhrp redirect
Router(config-if)# tunnel source Serial1/0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel key 100000
Router(config-if)# tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
ip nhrp redirect	Enables NHRP redirect.

ip nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ip nhrp trigger-svc** command in interface configuration mode. To restore the default thresholds, use the **no** form of this command.

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

no ip nhrp trigger-svc

Syntax Description

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

Defaults

trigger-threshold: 1 kbps

teardown-threshold: 0 kbps

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default. To change that interval, use the **load-interval** *seconds* argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kbps and 5 kbps, respectively:

```
ip nhrp trigger-svc 100 5
```

Related Commands

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

ip nhrp use

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

ip nhrp use *usage-count*

no ip nhrp use *usage-count*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally sent immediately. Configuring the *usage-count* argument causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 10.0.0.1 and one packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ip nhrp use 5
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

show ip nhrp

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

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

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See Table 46 for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See Table 46 for types, number ranges, and descriptions.
static	(Optional) Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ip nhrp map** command. See Table 46 for types, number ranges, and descriptions.
address	(Optional) Displays NHRP mapping entries for specified protocol addresses.
interface	(Optional) Displays NHRP mapping entries for the specified interface. See Table 46 for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.
shortcut	(Optional) Displays NHRP shortcut information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command Default

Information is displayed for all NHRP mappings.

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The output of this command was extended to display the NHRP group received from the spoke.
Cisco IOS XE Release 2.5	This command was modified. Support was added for the **shortcut** keyword.

Usage Guidelines

Table 46 lists the valid types, number ranges, and descriptions for the optional *interface* argument.

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

Table 46 Valid Types, Number Ranges, and Interface Description

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

Examples

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

```
Router# show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:17:49, expire 00:01:30
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-0
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:11, expire 01:59:48
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.3
  Group: test-group-0
11.0.0.2/32 via 11.0.0.2, Tunnel1 created 00:17:49, expire 00:02:10
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-1
```

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

```
Router#show ip nhrp shortcut

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

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

```
Router# show ip nhrp detail

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

Table 47 describes the significant fields shown in the displays.

Table 47 show ip nhrp Field Descriptions

Field	Description
10.1.1.1/8	Target network.
via 10.2.1.1	Next Hop to reach the target network.
Tunnel1	Interface through which the target network is reached.
created 00:00:12	Length of time since the entry was created (hours:minutes:seconds).
expire 01:59:47	Time remaining until the entry expires (hours:minutes:seconds).
never expire	Indicates that static entries never expire.
Type	• dynamic—NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static—NHRP mapping is configured statically. Entries configured by the **ip nhrp map** command are marked static. • incomplete—The NBMA address is not known for the target network.
NBMA address	Nonbroadcast multiaccess address of the next hop. The address format is appropriate for the type of network being used: ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel.

Table 47 show ip nhrp Field Descriptions (continued)

Field	Description
Flags	• authoritative—Indicates that the NHRP information was obtained directly from the Next Hop Server or router that maintains and is authoritative for the NBMA-to-IP address mapping for a particular destination. • implicit—Indicates that the local node learned about the NHRP mapping entries from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router. • local—Indicates NHRP mapping entries that are for networks local to this router (that is, serviced by this router). These flag entries are created when this router answers an NHRP resolution request that has this information and is used to store the transport (tunnel) IP address of all the other NHRP nodes to which it has sent this information. If for some reason this router loses access to this local network (that is, it can no longer service this network), it sends an NHRP purge message to all remote NHRP nodes that are listed in the "local" entry (in **show ip nhrp detail** command output) to tell the remote nodes to clear this information from their NHRP mapping tables. This local mapping entry times out of the local NHRP mapping database at the same time that this information (from the NHRP resolution reply) would time out of the NHRP mapping database on the remote NHRP nodes. • nat—Indicates that the remote node (NHS client) supports the new NHRP NAT extension type for dynamic spoke-spoke tunnels to/from spokes behind a NAT router. This marking does not indicate that the spoke (NHS client) is behind a NAT router.

Table 47 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	• negative—For negative caching, indicates that the requested NBMA mapping has not yet been or could not be obtained. When NHRP sends an NHRP resolution request, an incomplete (negative) NHRP mapping entry for the address is inserted in the resolution request. This insertion suppresses any more triggering of NHRP resolution requests while the resolution request is being resolved. If configured, any encryption parameters (IKE/IPsec) for the tunnel are negotiated. • (no socket)—Indicates that the NHRP mapping entries will not trigger IPsec to set up encryption because data traffic does not need to use this tunnel. Later, if data traffic needs to use this tunnel, the flag will change from a “(no socket)” to a “(socket)” entry and IPsec will be triggered to set up the encryption for this tunnel. Local and implicit NHRP mapping entries are always initially marked as “(no socket).” By default, NHRP caches source information from NHRP resolution request or replies as they go through the system. To allow this caching to continue, but not have the entry create an IPsec socket, they are marked as (no socket). If this was not done there would be extra IPsec sockets from the hubs to the various spokes that either were not used or were used for only one or two packets while a direct spoke-to-spoke tunnel was being built. Data packets and NHRP packets that arrive on the tunnel interface and are forwarded back out the tunnel interface are not allowed to use the (no socket) NHRP mappings for forwarding. Because, in this case, the router is an intermediate node in the path between the two endpoints and we only want to create short-cut tunnels between the initial entrance and final exit point of the DMVPN (NBMA) network and not between any intermediate nodes. If at some point the router receives a data packet that has a source interface that is not the tunnel interface and it would use the (no socket) mapping entry, the router converts the (no socket) entry to a (socket) entry. In this case, this router is the entrance (or exit) point of the NBMA (for this traffic stream).

Table 47 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	• (no socket) (continued)—These (no socket) mapping entries are marked (non-authoritative); only mappings from NHRP registrations are marked (authoritative). The NHRP resolution requests are also marked (authoritative), which means that the NHRP resolution request can be answered only from an (authoritative) NHRP mapping entry. A (no socket) mapping entry will not be used to answer an NHRP resolution request and the NHRP resolution request will be forwarded to the NHS of the nodes . • registered—Indicates that the mapping entry was created in response to an NHRP registration request. Although registered mapping entries are dynamic entries, they may not be refreshed through the “used” mechanism. Instead, these entries are refreshed by another NHRP registration request with the same transport (tunnel) IP to NBMA address mapping. The Next Hop Client (NHC) periodically sends NHRP registration requests to keep these mappings from expiring. • router—Indicates that NHRP mapping entries for a remote router (that is accessing a network or host behind the remote router) are marked with the router flag. • unique—NHRP registration requests have the unique flag set on by default. This flag indicates that an NHRP mapping entry cannot be overwritten by a mapping entry that has the same IP address and a different NBMA address. When a spoke has a statically configured outside IP (NBMA) address, this is used to keep another spoke that is mis-configured with the same transport (tunnel) IP address from overwriting this entry. If a spoke has a dynamic outside IP (NBMA) address, you can configure the **ip nhrp registration no-unique** command on the spoke to clear this flag. This configuration allows the registered NHRP mapping entry for that spoke on the hub to be overwritten with a new NBMA address. This is necessary in this case because the spoke's outside IP (NBMA) address can change at any time. If the “unique” flag was set, the spoke would have to wait for the mapping entry on the hub to time out before it could register its new (NBMA) mapping.

Table 47 show ip nhrp Field Descriptions (continued)

Field	Description
Flags (continued)	• used—When data packets are process-switched and this mapping entry was used, the mapping entry is marked as used. The mapping database is checked every 60 seconds. If the used flag is set and more than 120 seconds remain until expire time, the used flag is cleared. If fewer than 120 seconds are left, this mapping entry is "refreshed" by the transmission of another NHRP resolution request. **Note** When using DMVPN Phase 3 in 12.4(6)T, CEF switched packets will also set the "used" flag, and these entries will be timed out and refreshed as described in the "used" flag description above.

Related Commands

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

show ip nhrp group-map

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

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

Syntax Description

group-name	(Optional) Name of an NHRP group mapping for which information will be displayed.

Command Default

Information is displayed for all NHRP group mappings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

 NHRP group: test-group-2
  QoS policy: p1
  Tunnels using the QoS policy: None
```

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

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

Table 48 describes the significant fields shown in the displays.

Table 48 show ip nhrp group-map Field Descriptions

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

Related Commands

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

show ip nhrp multicast

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

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

Syntax Description

nbma-address	(Optional) Displays multicast mapping information for the specified NBMA address.
interface	(Optional) Displays all multicast mapping entries of the NHRP network for the interface. See Table 49 for types, number ranges, and descriptions.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(7)	This command was introduced.

Usage Guidelines

Table 49 lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note

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

Table 49 Valid Types, Number Ranges, and Interface Descriptions

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

Table 49 Valid Types, Number Ranges, and Interface Descriptions (continued)

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

Examples

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

```
Router# show ip nhrp multicast

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

Table 50 describes the fields shown in the display.

Table 50 show ip nhrp Field Descriptions

Field	Description
I/F	Interface associated with the multicast mapping entry.
NBMA address	Nonbroadcast Multiaccess Address to which multicast packets will be sent. The address format is appropriate for the type of network used: ATM, Ethernet, SMDS, or multipoint tunnel.
Flags	• static—Indicates that the multicast mapping entry is configured statically by the **ip nhrp map multicast** command. • dynamic—Indicates that the multicast mapping entry is obtained dynamically. A multicast mapping entry is created for each registered Next Hop Client (NHC) when the **ip nhrp map multicast dynamic** command is configured.

Related Commands

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

show ip nhrp nhs

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

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

Syntax Description

interface-type	(Optional) Type of interface for which NHS information should be displayed. See Table 49 for types, number ranges, and descriptions.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays NHS recovery information.
cluster *number*	(Optional) Displays NHS recovery information based on the cluster value. The range is from 0 to 10.
preempted	(Optional) Displays NHSs that are declared as down and not actively probed.
running	(Optional) Displays NHSs that are responding or expecting replies.
waiting	(Optional) Displays NHSs that are waiting to be scheduled.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **redundancy**, **cluster** *number*, **preempted**, **running**, and **waiting** keywords and argument were added.

Usage Guidelines

Table 51 lists the valid types, number ranges, and descriptions for the optional *interface-number* argument.

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

Table 51 Valid Types, Number Ranges, and Interface Descriptions

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

Examples

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

```
Router# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding

Tunnel1:
  10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0

Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

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

```
Router# show ip nhrp nhs

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
192.0.2.1  W priority = 2 cluster = 0
192.0.2.2  RE priority = 0 cluster = 0
192.0.2.3  RE priority = 1 cluster = 0
```

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

```
Router# show ip nhrp nhs redundancy

Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS         Priority  Cur-State  Cur-Queue  Prev-State Prev-Queue
1    Tunnel0    0        10.0.0.253  3         RE         Running    E          Running
2    Tunnel0    0        10.0.0.252  2         RE         Running    E          Running
3    Tunnel0    0        10.0.0.251  1         RE         Running    E          Running

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

Table 50 describes the significant fields shown in the displays.

Table 52   show ip nhrp nhs Field Descriptions

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

Related Commands

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

show ip nhrp summary

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

show ip nhrp summary

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

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

```
Router# show ip nhrp summary

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

Table 53 describes the significant field shown in the display.

Table 53 show ip nhrp summary Field Descriptions

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

Related Commands

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

show ip nhrp traffic

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

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

Syntax Description

interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	(Optional) Specifies the tunnel interface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.4(6)T	The command output was enhanced to display traffic indication packets (redirects).
12.4(9)T	The **interface** and **tunnel** keywords and the *number* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
Router# show ip nhrp traffic interface tunnel0

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

Table 54 describes the significant fields shown in the display.

Table 54 show ip nhrp traffic Field Descriptions

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

Table 54 show ip nhrp traffic Field Descriptions (continued)

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

Related Commands

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

show nhrp debug-condition

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

show nhrp debug-condition

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show nhrp debug-condition

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

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

Related Commands

Command	Description
debug nhrp condition	Enables the NHRP conditional debugging.