



ip arp inspection vlan through lease

- [ip arp inspection vlan, page 3](#)
- [ip arp inspection vlan logging, page 5](#)
- [ip arp proxy disable, page 7](#)
- [ip default-gateway, page 8](#)
- [ip dhcp bootp ignore, page 10](#)
- [ip dhcp class, page 11](#)
- [ip dhcp conflict logging, page 13](#)
- [ip dhcp database, page 15](#)
- [ip dhcp excluded-address, page 17](#)
- [ip dhcp ping packets, page 19](#)
- [ip dhcp ping timeout, page 21](#)
- [ip dhcp pool, page 23](#)
- [ip dhcp snooping, page 25](#)
- [ip dhcp snooping binding, page 27](#)
- [ip dhcp snooping database, page 29](#)
- [ip dhcp snooping information option, page 31](#)
- [ip dhcp snooping limit rate, page 33](#)
- [ip dhcp snooping verify mac-address, page 35](#)
- [ip dhcp snooping vlan, page 37](#)
- [ip dhcp use, page 39](#)
- [ip domain list, page 41](#)
- [ip domain lookup, page 43](#)
- [ip domain name, page 45](#)
- [ip name-server, page 47](#)

- [ip proxy-arp, page 49](#)
- [ip route, page 50](#)
- [ip routing, page 55](#)
- [ip source binding, page 56](#)
- [ip verify source vlan dhcp-snooping, page 58](#)
- [ipv6 address dhcp, page 60](#)
- [ipv6 dhcp guard attach-policy, page 62](#)
- [ipv6 dhcp ping packets, page 64](#)
- [ipv6 dhcp pool, page 66](#)
- [ipv6 dhcp server, page 69](#)
- [lease, page 72](#)

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

<i>vlan-range</i>	VLAN number or range; valid values are from 1 to 4094.
-------------------	--

Command Default

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.

Command	Description
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

<i>vlan-range</i>	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.

Command Default 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.

Release	Modification
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 reen able 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 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

<i>ip-address</i>	IP address of the router.
-------------------	---------------------------

Command Default

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.

Command	Description
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 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.

Command Default 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

<i>class-name</i>	Name of the DHCP class.
-------------------	-------------------------

Command Default

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 01030a0b0c020500000000123
  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 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.

Command Default 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.

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

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

<i>url</i>	Specifies the remote file used to store the automatic bindings. The following are acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
timeout <i>seconds</i>	(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 <i>seconds</i>	(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.

Command Default

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.

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.

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.
<i>vrf-name</i>	(Optional) The VRF name.
<i>ip-address</i>	The excluded IP address, or first IP address in an excluded address range.
<i>last-ip-address</i>	(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 <i>vrf-name</i> 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 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

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

Command Default

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

<i>milliseconds</i>	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.
---------------------	---

Command Default

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

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

Command Default

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.

Command	Description
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 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.

Command Default 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.

Command	Description
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

<i>mac-address</i>	MAC address.
vlan <i>vlan</i>	Specifies a valid VLAN number; valid values are from 1 to 4094.
<i>ip-address</i>	IP address.
interface <i>type</i>	Specifies the interface type; possible valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet .
<i>number</i>	Module and port number.
expiry <i>seconds</i>	Specifies the interval after which binding is no longer valid; valid values are from 1 to 4294967295 seconds.

Command Default

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: <i>url</i>	Specifies the database URL for storing entries using the bootflash.
ftp: <i>url</i>	Specifies the database URL for storing entries using FTP.
rcp: <i>url</i>	Specifies the database URL for storing entries using remote copy (rcp).
scp: <i>url</i>	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: <i>url</i>	Specifies the database URL for storing entries using TFTP.
timeout <i>seconds</i>	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay <i>seconds</i>	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.

Command Default

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.

Release	Modification
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.
------------------------	---

Command Default

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

<i>rate</i>	Number of DHCP messages that a switch can receive per second; valid values are from 1 to 4294967294 seconds.
-------------	--

Command Default

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 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.

Command Default 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.

Command	Description
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

<i>number</i> <i>vlan-list</i>	VLAN number or a group of VLANs; valid values are from 1 to 4094. See the “Usage Guidelines” section for additional information.
----------------------------------	--

Command Default

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 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.

Release	Modification
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 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 <i>vrf-name</i>	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The <i>vrf-name</i> argument specifies a name for the VRF table.
<i>name</i>	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

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 <i>vrf-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.
<i>interface-type interface-number</i>	(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 noform of this command.

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

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

Syntax Description

vrf <i>vrf-name</i>	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The <i>vrf-name</i> argument specifies a name for the VRF table.
<i>name</i>	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

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 <i>vrf-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 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 <i>vrf-name</i>	(Optional) Defines a Virtual Private Network (VPN) routing and forwarding instance (VRF) table. The <i>vrf-name</i> argument specifies a name for the VRF table.
<i>server-address1</i>	IPv4 or IPv6 addresses of a name server.
<i>server-address2...server-address6</i>	(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 <i>vrf-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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).

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.

Command Default 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 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 <i>vrf-name</i>	(Optional) Configures the name of the VRF by which static routes should be specified.
<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	Prefix mask for the destination.
<i>ip-address</i>	IP address of the next hop that can be used to reach that network.
<i>interface-type interface-number</i>	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.
<i>distance</i>	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name <i>next-hop-name</i>	(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 <i>number</i>	(Optional) Associates a track object with this route. Valid values for the <i>number</i> argument range from 1 to 500.
tag <i>tag</i>	(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 <i>number</i> argument were added.
12.3(8)T	The track keyword and <i>number</i> argument were integrated into Cisco IOS Release 12.3(8)T. The dhcp keyword was added.
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 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.

Command Default IP routing is enabled.

Command Modes Global configuration (config)

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.

Disabling IP routing is not allowed if you are running Cisco IOS Release 12.2SX on a Catalyst 6000 platform. The workaround is to not assign an IP address to the SVI.

Examples The following example enables IP routing:

```
Router# configure terminal
Router(config
)
# 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

<i>mac-address</i>	Binding MAC address.
vlan <i>vlan-id</i>	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
<i>ip-address</i>	Binding IP address.
interface <i>type</i>	Interface type; possible valid values are fastethernet , gigabitethernet , tengigabitethernet , port-channel num , and vlan <i>vlan-id</i> .
<i>mod / port</i>	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 00C.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 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 ethernet
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.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.
---------------------	---

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode

```
ipv6 dhcp guard [attach-policy [ policy-name ]] [vlan {add|all|except|none|remove} vlan-id [... vlan-id]]
```

```
no ipv6 dhcp guard [attach-policy [ policy-name ]] [vlan {add|all|except|none|remove} vlan-id [... vlan-id]]
```

Syntax Available In VLAN Configuration Mode

```
ipv6 dhcp guard attach-policy [ policy-name ]
```

```
no ipv6 dhcp guard attach-policy [ policy-name ]
```

Syntax Description

<i>policy-name</i>	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
<i>vlan-id</i>	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default No DHCPv6 guard policy is attached.

Command Modes Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy poll vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*

ipv6 dhcp ping packets

Syntax Description

<i>number</i>	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.
---------------	---

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the 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 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

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

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

Syntax Description

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

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
 - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

**Note**

The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named `cisco1` and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool `cisco1`:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named `engineering` with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named `350` with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
```

```
Router(config-dhcpv6)# vendor-specific 9  
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1  
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"  
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [*poolname*] **automatic**] [**rapid-commit**] [**preference value**] [**allow-hint**]
no ipv6 dhcp server

Syntax Description

<i>poolname</i>	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference value	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The automatic keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

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

<i>days</i>	Specifies the duration of the lease in numbers of days.
<i>hours</i>	(Optional) Specifies the number of hours in the lease. A <i>days</i> value must be supplied before you can configure an <i>hours</i> value.
<i>minutes</i>	(Optional) Specifies the number of minutes in the lease. A <i>days</i> value and an <i>hours</i> value must be supplied before you can configure a <i>minutes</i> value.
infinite	Specifies that the duration of the lease is unlimited.

Command Default

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.

