

ip dhcp ping timeout through ip dhcp-client forcerenew

- ip dhcp ping timeout, on page 3
- ip dhcp pool, on page 4
- ip dhcp relay bootp ignore, on page 6
- ip dhcp relay prefer known-good-server , on page 7
- ip dhcp relay forward spanning-tree, on page 8
- ip dhcp relay information check, on page 9
- ip dhcp relay information check-reply, on page 10
- ip dhcp relay information option, on page 12
- ip dhcp relay information option server-id-override, on page 15
- ip dhcp relay information option subscriber-id, on page 17
- ip dhcp relay information option vpn-id, on page 19
- ip dhcp relay information option-insert, on page 21
- ip dhcp relay information policy, on page 23
- ip dhcp relay information policy-action, on page 25
- ip dhcp relay information trust-all, on page 27
- ip dhcp relay information trusted, on page 28
- ip dhcp-relay source-interface, on page 29
- ip dhcp route connected, on page 30
- ip dhcp server use subscriber-id client-id, on page 31
- ip dhcp smart-relay, on page 32
- ip dhcp snooping, on page 33
- ip dhcp snooping binding, on page 34
- ip dhcp snooping database, on page 35
- ip dhcp snooping detect spurious, on page 37
- ip dhcp snooping detect spurious interval, on page 39
- ip dhcp snooping detect spurious vlan, on page 40
- ip dhcp snooping glean, on page 41
- ip dhcp snooping information option, on page 42
- ip dhcp snooping limit rate, on page 44
- ip dhcp snooping packets, on page 46
- ip dhcp snooping verify mac-address, on page 47

- ip dhcp snooping vlan, on page 48
- ip dhcp subscriber-id interface-name, on page 49
- **ip dhcp support option55-override** , on page 50
- ip dhcp support tunnel unicast, on page 51
- ip dhcp update dns, on page 52
- ip dhcp use, on page 53
- ip dhcp use subscriber-id client-id, on page 55
- ip dhcp-client broadcast-flag, on page 56
- ip dhcp-client default-router distance, on page 57
- ip dhcp-client forcerenew, on page 58

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.

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*

Note When configuring the **ip dhcp pool** command, note that it can be affected by the **ip dhcp database** command if an incorrect URL is provided. The console may hang due to multiple attempts by the DHCP service to reach the URL before it returns a failure. This is expected behavior. To prevent this issue, ensure that the correct URL, including the file name, is provided when using the **ip dhcp database** command, especially when it includes ftp/tftp.

Syntax Description

name	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.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.

Command	Description
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 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 forward spanning-tree

To set the gateway address (giaddr) field in the DHCP packet before forwarding to spanning-tree interfaces, use the **ip dhcp relay forward spanning-tree** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp relay forward spanning-tree
no ip dhcp relay forward spanning-tree

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Prior to Cisco IOS Release 12.1, when the **ip forward-protocol spanning-tree any-local-broadcast** command was configured, DHCP broadcasts were forwarded to all spanning-tree enabled interfaces after setting the giaddr field in the DHCP packet.

The behavior of the DHCP relay agent was modified in release 12.1 such that the DHCP broadcasts were still forwarded to all spanning-tree enabled interfaces but the giaddr field was not set on the packets. This behavior can cause problems in a network because the DHCP server uses the giaddr field to properly allocate addresses when the client is not in the local network.

Use the **ip dhcp relay forward spanning-tree** command to set the giaddr to the IP address of the incoming interface before forwarding DHCP broadcasts to spanning-tree enabled interfaces.

The **ip forward-protocol udp** command is enabled by default and automatically determines that BOOTP client and server datagrams (ports 67 and 68) should be forwarded. This forwarding results in another packet sent to spanning-tree enabled interfaces without the giaddr field set. To avoid these duplicate packets, use the **no ip forward-protocol udp bootpc** and **no ip forward-protocol udp bootps** commands.

Examples

In the following example, the giaddr field in the DHCP packet will be set to the IP address of the incoming interface before forwarding to spanning-tree enabled interfaces:

```
ip dhcp relay forward spanning-tree
ip forward-protocol spanning-tree any-local-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets
ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

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.

Command Default

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.

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.

Command	Description
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**commandis 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
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 helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

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 Dynamic Host Configuration Protocol (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 command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp relay information option server-id-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** 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 Ethernet interface 0/0:

```
Device(config)# interface Ethernet0/0
Device(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 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.

Command Default

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 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.

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.

Command	Description
ip dhcp relay information policy-action	Configures the information reforwarding policy for a DHCP relay agent.

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.

Command Default

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.

Command Default

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 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 this 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 command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** 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** command is also configured, the **ip dhcp relay source-interface** 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:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(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.

Command Default

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 use subscriber-id client-id

To configure the Dynamic Host Configuration Protocol (DHCP) server to use the subscriber identifier as the client identifier on all incoming DHCP messages on an interface, use the **ip dhcp server use subscriber-id client-id** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp server use subscriber-id client-id
no ip dhcp server 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

Interface configuration (config-if)

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 takes precedence on the interface over the **ip dhcp use subscriber-id client-id** command.

Examples

In the following example, the DHCP server uses the subscriber identifier as the client identifier for all incoming messages received on Ethernet interface 0/0:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip dhcp server use subscriber-id client-id
```

Related Commands

Command	Description
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.

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.

Command Default

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.

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.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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.

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: *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.

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.
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 detect spurious

To enable spurious DHCP server detection on a VLAN, use the **ip dhcp snooping detect spurious vlan** command in global configuration mode. To disable spurious DHCP server detection on a VLAN, use the **no** form of this command.

ip dhcp snooping detect spurious vlan *word*
no ip dhcp snooping detect spurious vlan *word*

Syntax Description

word	DHCP snooping VLAN or VLAN range.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to enable spurious DHCP server detection on a specified VLAN list:

```
Router(config)# ip dhcp snooping detect spurious vlan 3-5
WORD DHCP Snooping vlan list number or vlan range, example: 1,3-5,7,9-11
Router(config)# ip dhcp snooping detect spurious interval ?
<1-65535> Time in minutes
```

Specify the interval between the DHCPDISCOVER messages.

```
Router# show ip dhcp snooping detect spurious ?

entry DHCP snooping detect spurious entry
| Output modifiers
<cr>
```

Provides brief configuration information related to spurious DHCP server detection.

```
Router# show ip dhcp snooping detect spurious entry ?

vlan spurious entry VLAN
| Output modifiers
<cr>
```

Displays all the learnt entries or those from a specific VLAN.

```
Router# clear ip dhcp snooping detect spurious entry ?

vlan Spurious entry VLAN
<cr>
```

Clears either all entries or those from a specific VLAN.

```
Router# show ip dhcp snooping detect spurious
```

```
Spurious DHCP server detection enabled
Detection VLAN list : 13-15,20,30
Detection interval : 10 minutes
Router# sh ip dhcp sn det sp en

Count  MacAddress       IpAddress       VLAN Interface               Last Seen
------ ---------------- --------------- ---- -----------             ------------
1      0004.2322.9dc9    20.0.0.1        20   GigabitEthernet1/25     Sep 21 2009 15:37:50

1      0004.2322.9dc9    10.78.96.194    20   GigabitEthernet1/25     Sep 21 2009 15:37:37

1      0011.955f.067c    30.0.0.1        30   GigabitEthernet1/26     Sep 21 2009 15:37:52
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious interval	Specifies the interval time between DHCPDISCOVER messages.
ip dhcp snooping detect spurious vlan	Enables spurious DHCP server detection on a VLAN.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping detect spurious interval

To set the interval time between DHCPDISCOVER messages, use the **ip dhcp snooping detect spurious interval** command in global configuration mode. To reset the time to its default time, use the **no** form of this command.

ip dhcp snooping detect spurious interval *time*
no ip dhcp snooping detect spurious

Syntax Description

time	Time in minutes between DHCPDISCOVER messages; valid values are 1 through 65535.

Command Default

30 minutes is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to set the time interval between DHCPDISCOVER messages to 350 minutes:

```
Router(config)# ip dhcp snooping detect spurious interval 350
Router(config)#
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious vlan	Enables spurious DHCP server detection on a VLAN.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping detect spurious vlan

To enable spurious DHCP server detection on a VLAN, use the **ip dhcp snooping detect spurious vlan** command in global configuration mode. To disable spurious DHCP server detection on a VLAN, use the **no** form of this command.

ip dhcp snooping detect spurious vlan *range*
no ip dhcp snooping detect spurious vlan *range*

Syntax Description

range	DHCP snooping VLAN or VLAN range.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXH6	Support for this command was introduced.

Examples

This example shows how to enable spurious DHCP server detection on a specified VLAN list:

```
Router(config)# ip dhcp snooping detect spurious vlan 3-5
Router(config)#
```

Related Commands

Command	Description
clear ip dhcp snooping detect spurious entry	Clears all entries or those from a specific VLAN.
ip dhcp snooping detect spurious interval	Specifies the interval time between DHCPDISCOVER messages.
show ip dhcp snooping detect spurious	Displays the configuration information related to spurious DHCP server detection.
show ip dhcp snooping detect spurious entry	Displays all the learnt entries or those from a specific VLAN.

ip dhcp snooping glean

To enable DHCP gleaning for a device, use the **ip dhcp snooping glean** command in global configuration mode. To disable DHCP gleaning, use the **no** form of this command.

ip dhcp snooping glean
no ip dhcp snooping glean

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP gleaning is disabled for a device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 15.2E	This command was introduced.

Usage Guidelines

DHCP gleaning is a read-only DHCP snooping functionality that allows components to register and glean DHCP version 4 packets. When you enable DHCP gleaning, it does a read-only snooping on all active interfaces on which DHCP snooping is disabled.

To know if DHCP gleaning is enabled on the device, use the **show ip dhcp snooping** command in privileged EXEC mode.

Examples

This example shows how to enable DHCP gleaning on a device and configure an interface as a trusted source for DHCP gleaning:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping glean
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# ip dhcp snooping trust
Device(config-if)# end
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping on a device.
show ip dhcp snooping	Displays DHCP snooping configuration information.

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 or template configuration mode. To remove the DHCP message rate limit, 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 device can receive per second; valid values are from 1 to 4294967294 seconds. When configuring using interface templates in template configuration mode, the range is from 1 to 2048 seconds.

Command Default

The DHCP snooping limit rate is not configured.

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.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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 device can receive per second:

```
Device(config-if)# ip dhcp snooping limit rate 150
```

This example shows how to disable the DHCP message rate limiting:

```
Device(config-if)# no ip dhcp snooping limit rate
```

The following example shows how to specify the number of DHCP messages that a device can receive per second using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# ip dhcp snooping limit rate 150
Device(config-template)# end
```

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.

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.

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.
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.
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 {*numbervlan-list*}
no ip dhcp snooping vlan {*numbervlan-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.

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 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 support option55-override

To enable a DHCP server to override multiple option 55 (parameter request list) requests sent by a DHCP client and send a DHCPOFFER message with all the sub-options set in the option 55, use the **ip dhcp support option55-override** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support option55-override
no ip dhcp support option55-override

Syntax Description

This command has no arguments or keywords.

Command Default

A DHCP server accepts the first instance of the option 55 request and ignores the remaining instances. Therefore, the server sends a DHCPOFFER message, which may not contain all the information required by the DHCP client

Command Modes

Global configuration (config)

Command History

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

Examples

The following example shows how to enable a DHCP server to override multiple option 55 requests:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp support option55-override
```

Related Commands

Command	Description
ip address dhcp	Acquires an interface IP address from the DHCP.
ip dhcp client request	Configures a DHCP client to request an option from a DHCP server.

ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the **ip dhcp support tunnel unicast** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support tunnel unicast
no ip dhcp support tunnel unicast

Syntax Description

This command has no arguments or keywords.

Command Default

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the **ip dhcp support tunnel unicast** command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCPOFFER and DHCPACK messages to the spoke.

Examples

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

Related Commands

Command	Description
ip address dhcp	Configures an IP address on an interface acquired through DHCP.
ip dhcp client broadcast-flag	Configures the DHCP client to set or clear the broadcast flag.

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.

Command Default

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 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-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.

Command Default

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 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.

Command Default

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.