ip arp gratuitous through ip dhcp ping packets

ip arp gratuitous

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

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

no ip arp gratuitous

Syntax Description

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

Command Default

Gratuitous ARP control is enabled.

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

Related Commands

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

ip arp incomplete

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

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

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

Syntax Description

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip arp inspection filter vlan

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

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

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

Syntax Description

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

Command Default

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

ip arp inspection limit (interface configuration)

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

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

no ip arp inspection limit

Syntax Description

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

Command Default

The default settings are as follows:

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

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

ip arp inspection log-buffer

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

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

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

Syntax Description

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

Command Default

The default settings are as follows:

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

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

Related Commands

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

ip arp inspection trust

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

ip arp inspection trust

no ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

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

Related Commands

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

ip arp inspection validate

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

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

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

Syntax Description

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

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

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

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

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

When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst**

mac validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

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

Examples

This example shows how to enable the source MAC validation:

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

Related Commands

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

ip arp inspection vlan

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

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

Syntax Description

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

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

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

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 poll

To configure the IP Address Resolution Protocol (ARP) polling for unnumbered interfaces, use the **ip arp poll** command in global configuration mode. To remove the IP ARP polling for unnumbered interfaces, use the **no** form of this command.

ip arp poll {**queue** *queue-size*| **rate** *packet-rate*}

no ip arp poll {**queue**| **rate**}

Syntax Description

queue *queue-size*	Configures the IP ARP polling queue size, in packets. The range is from 0 to 10000. The default is 1000.
rate *packet-rate*	Configures the IP ARP polling packet rate, in packets per second. The range is from 0 to 10000. The default is 1000.

Command Default

IP ARP polling for unnumbered interfaces has a default queue size of 1000 and packet rate of 1000 packets per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following example shows how to configure the queue size for IP ARP polling for unnumbered interfaces:

```
Device(config)# ip arp poll queue 5000
```

The following example shows how to configure the packet rate for IP ARP polling for unnumbered interfaces:

```
Device(config)# ip arp poll rate 5000
```

Related Commands

Command	Description
show ip arp poll	Displays the IP ARP host polling status.

ip arp proxy disable

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

ip arp proxy disable

no ip arp proxy disable

Syntax Description

This command has no arguments or keywords.

Command Default

Proxy ARP is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example disables proxy ARP:

```
ip arp proxy disable
```

The following example enables proxy ARP:

```
no ip arp proxy disable
```

Related Commands

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

ip arp queue

To configure the Address Resolution Protocol (ARP) input packet queue size, use the **ip arp queue** command in global configuration mode. To restore the default, use the **no** form of this command.

ip arp queue *queue-size*

no ip arp queue

Syntax Description

queue-size	Size of the ARP input packet queue. Valid values are from 512 to 2147483647.

Command Default

By default, the queue size is configured as 512.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M5	This command was introduced.

Usage Guidelines

You can configure the ARP input packet queue size based on the volume of the incoming traffic. The ARP input queue size can be set by the platform during initialization. The ARP input packet size is configurable at the system level but not at the interface level.

Examples

The following example shows how to configure the ARP input packet queue size as 650:

```
Router(config)# ip arp queue 650
```

ip classless

To enable a router to forward packets, which are destined for a subnet of a network that has no network default route, to the best supernet route possible, use the **ip classless** command in global configuration mode. To disable the functionality, use the **no**form of this command.

ip classless

no ip classless

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table, and there is no network default route.

Note If the supernet or default route is learned by using Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), the **no ip classless** configuration command is ignored.

Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip ddns update hostname

To enable a host to be used for Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **ip ddns update hostname**command in interface configuration mode. To disable the dynamic updates, use the **no** form of this command.

ip ddns update hostname *hostname*

no ip ddns update hostname *hostname*

Syntax Description

hostname	Specifies a hostname of the server that will receive updates. **Note** It is expected that the hostname will be an fully qualified domain name (FQDN). Using an FQDN hostname enables the specification of a hostname in a different domain that the default domain of the device.

Command Default

No host is configured.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to configure the testhost host to update A and PTR RRs:

```
interface ethernet1/0
 ip ddns update hostname testhost
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip ddns update method

To specify a method and method name for updating Dynamic Domain Name System (DDNS) address (A) and pointer (PTR) Resource Records (RRs) and enter DDNS-update-method configuration mode, use the **ip ddns update method**command in global configuration mode. To disable the dynamic updating, use the **no** form of this command.

ip ddns update method *method-name*

no ip ddns update method

Syntax Description

method-name	IETF standardized DDNS update method name.

Command Default

No DDNS update method is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The interface configuration overrides the global configuration.

Examples

The following example shows how to assign a DDNS update method name:

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

Once you have assigned the method name, you can specify the type of update (DDNS or HTTP) and set a maximum interval. Refer to the **ddns** and **http** commands for more information.

Related Commands

Command	Description
ddns	Specifies DDNS as the update method for A and PTR RRs.
http	Specifies HTTP as the update method for A and PTR RRs.

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** command in global configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the router.

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 redirectmessage 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 aaa default username

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

ip dhcp aaa default username *name*

no ip dhcp aaa default username *name*

Syntax Description

name	Name of the address pool.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ip dhcp bootp ignore

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

ip dhcp bootp ignore

no ip dhcp bootp ignore

Syntax Description

This command has no arguments or keywords.

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

class-name	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 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 00000000000000000000FF
ip dhcp class CLASS2
 relay agent information
! Relay agent information patterns
  relay-information hex 01040102030402020102
  relay-information hex 01040101030402020102
```

```
ip dhcp class CLASS3
 relay agent information
```

Related Commands

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

ip dhcp client

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

ip dhcp client route track *number*

no ip dhcp client route track

Syntax Description

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

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp client authentication key-chain

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

ip dhcp client authentication key-chain *name* **[forcerenew]**

no ip dhcp client authentication key-chain

Syntax Description

name	Name of the key chain.
forcerenew	(Optional) Configures DHCP authentication only for FORCERENEW messages.

Command Default

Authentication is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(4)M	This command was modified. The **forcerenew** keyword was added.

Usage Guidelines

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

When the **ip dhcp client authentication key-chain** command is configured, authentication is enabled for all the DHCP messages including FORCERENEW messages that are received through the interface. To configure DHCP authentication only for the FORCERENEW messages, use **forcerenew** keyword.

Examples

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

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

Related Commands

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

ip dhcp client authentication mode

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

ip dhcp client authentication mode {**md5**| **token**} **[forcerenew]**

no ip dhcp client authentication mode

Syntax Description

md5	Specifies MD5-based authentication.
token	Specifies token-based authentication.
forcerenew	(Optional) Configures DHCP authentication only for FORCERENEW messages.

Command Default

No authentication mode is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(4)M	This command was modified. The **forcerenew** keyword was added.

Usage Guidelines

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

When the **ip dhcp client authentication key-chain** command is configured, authentication is enabled for all the DHCP messages including FORCERENEW messages that are received through the interface. To configure DHCP authentication only for FORCERENEW messages, use the **forcerenew** keyword.

Examples

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

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

Related Commands

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

ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the **ip dhcp client broadcast-flag** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client broadcast-flag {**clear**| **set**}

no ip dhcp client broadcast-flag

Syntax Description

clear	Clears the broadcast flag.
set	Sets the broadcast flag.

Command Default

The broadcast flag is set.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the **ip dhcp client broadcast-flag** command to configure the DHCP client to set or clear the broadcast flag.

Examples

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP.
ip dhcp support tunnel unicast	Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.

ip dhcp client class-id

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

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

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

Syntax Description

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

Command Default

No class identifier is specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip dhcp client client-id

To specify a client identifier and override the default client identifier, use the **ip dhcp client client-id** command in interface configuration mode. To return to the default form, use the **no** form of this command.

ip dhcp client client-id {*interface-name*| **ascii** *string*| **hex** *string*| **reuse-mac**}

no ip dhcp client client-id {*interface-name*| **ascii** *string*| **hex** *string*| **reuse-mac**}

Syntax Description

interface-name	Interface from which the MAC address is used.
ascii *string*	Specifies a unique ASCII string. The default value is cisco-*mac-name* where *mac* is the MAC address of the interface and 'name' is the short form of the interface name.
hex *string*	Specifies a unique hexadecimal value.
reuse-mac	Reuses the MAC address configured by the **atm ether-mac-address** command. **Note** The **reuse-mac** keyword is to be used only on ATM subinterfaces along with the **atm ether-mac-address** command.

Command Default

The client identifier is an ASCII value in the form cisco-*mac-name* where *mac* is the MAC address of the interface and *name* is the short form of the interface name.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(4)M4	This command was modified and integrated into Cisco IOS Release 15.1(4)M4. The **reuse-mac** keyword was added.

Usage Guidelines

The **ip dhcp client client-id** command is specified only when an IP address is acquired from a DHCP server. If the command is specified after an IP address has been acquired from the DHCP server, the command will

not take effect until the next time the device acquires an IP address from the DHCP server. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been specified.

When the **no** form of this command is specified, the configuration is removed and the system returns to the default form. To configure the system, a client identifier must be included.

Examples

The following example shows how to configure a client identifier named test-client-id:

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet 1
Device(config-if)# ip dhcp client client-id ascii test-client-id
```

Related Commands

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

ip dhcp client default-router distance

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

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

no ip dhcp client default-router distance

Syntax Description

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

Command Default

The default administrative distance is 254.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
debug dhcp client	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
ip dhcp-client default-router distance	Configures a default DHCP administrative distance for clients in global configuration mode.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp client hostname

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

ip dhcp client hostname *host-name*

no ip dhcp client hostname *host-name*

Syntax Description

host-name	Name of the host.

Command Default

The hostname is the globally configured hostname of the router.

Command Modes

Interface configuration(config-if)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

Command	Description
release dhcp	Performs an immediate release of a DHCP lease for an interface.
renew dhcp	Performs an immediate renewal of a DHCP lease for an interface.

ip dhcp client lease

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

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

no ip dhcp client lease

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows a one-day lease:

```
ip dhcp client lease 1
```

The following example shows a one-hour lease:

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

The following example shows a one-minute lease:

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

Related Commands

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

ip dhcp client mobile renew

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp client request

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

ip dhcp client request *option-name*

no ip dhcp client request *option-name*

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

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

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ip dhcp client route

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

ip dhcp client route track *number*

no ip dhcp client route track

Syntax Description

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

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp client update dns

To enable Dynamic Domain Name System (DDNS) updates of address (A) Resource Records (RRs) using the same hostname passed in the hostname and fully qualified domain name (FQDN) options by a client, use the **ip dhcp client update dns** command in interface configuration mode. To disable dynamic updates of A RRs, use the **no** form of this command.

ip dhcp client update dns [**server** {**both**| **none**}]

no ip dhcp client update dns [**server** {**both**| **none**}]

Syntax Description

server	(Optional) Specifies that the client will include an FQDN option specifying the "N" flag. The server will not perform any DDNS updates for the client. The server can, of course, override this configuration and do the updates anyway. • **both** --Enables the DHCP client to perform DDNS updates on both A (forward) and PTR (reverse) RRs in the primary DNS server unless the DHCP server has specified in the DHCP ACK FQDN option that it has overridden the client request and has updated the information previously. **Note** If the **both** keyword is specified, it means that the client will include an FQDN option specifying the S flag. This keyword instructs the server that it should attempt to dynamically update both the A and PTR RRs. • **none** --On the client side, specifies that the DHCP client should include the FQDN option; however, it should not attempt any DDNS updates. **Note** If the **none** keyword is not specified, the FQDN option will result in the server updating the PTR RR and neither the server nor the client will update the A RR.

Command Default

No default behavior.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Commands that are configured in interface configuration mode override the commands configured using global configuration mode. The **ip dhcp-client update dns** command (hyphenated) is the global configuration command.

If you specify the **both** and **none** keywords in separate configurations, the DHCP client will update both the A and PTR RRs, and the DHCP server will not perform any updates. If you specify the **none** and **both** keywords (in this order), the DHCP client will not perform any updates and the server will update both the A and PTR RRs.

There are two parts to the DDNS update configuration on the client side. First, if the **ip ddns update method** command is configured on the client, which specifies the DDNS-style updates, then the client will be trying to generate or perform A updates. If the **ip ddns update method ddns both** command is configured, then the client will be trying to update both A and PTR RRs.

Second, the only way for the client to communicate with the server, with reference to what updates it is generating or expecting the server to generate, is to include an FQDN option when communicating with the server. Whether or not this option is included is controlled on the client side by the **ip dhcp-client update dns** command in global configuration mode or the **ip dhcp client update dns** command in interface configuration mode.

Even if the client instructs the server to update both or update none, the server can override the client request and do whatever it was configured to do anyway. If there is an FQDN option in the DHCP interaction as above, then the server can communicate to the client that it was overridden, in which case the client will not perform the updates because it knows that the server has done the updates. Even if the server is configured to perform the updates after sending the ACK (the default), it can still use the FQDN option to instruct the client what updates it will be performing and thus the client will not do the same types of updates.

If the server is configured with the **update dns** command with or without any keywords, and if the server does not see an FQDN option in the DHCP interaction, then it will assume that the client does not understand DDNS and will automatically act as though it were configured to update both A and PTR RRs on behalf of the client.

Examples

The following example shows how to configure the DHCP client to perform A and PTR RR updates, but the DHCP server will not perform the updates:

```
ip dhcp client update dns server none
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

ip dhcp compatibility lease-query client

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

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

no ip dhcp compatibility lease-query client

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SCE1	This command was integrated into Cisco IOS Release 12.2(33)SCE1.

Usage Guidelines

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

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

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

- DHCPLEASEUNASSIGNED 11
- DHCPLEASEUNKNOWN 12
- DHCPLEASEACTIVE 13

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

Examples

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

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

Related Commands

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

ip dhcp compatibility suboption link-selection

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

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

no ip dhcp compatibility suboption link-selection

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp conflict logging

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

ip dhcp conflict logging

no ip dhcp conflict logging

Syntax Description

This command has no arguments or keywords.

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 conflict resolution

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

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

no ip dhcp conflict resolution

Syntax Description

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

Command Default

DHCP address conflict resolution is disabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip dhcp database

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

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

no ip dhcp database *url*

Syntax Description

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

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 debug ascii-client-id

To display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output, use the **ip dhcp debug ascii-client-id** command in global configuration mode. To disable To disable display of the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output, use the **no** form of this command.

ip dhcp debug ascii-client-id

no ip dhcp debug ascii-client-id

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP debug outputs do not display the client ID in ASCII format.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **ip dhcp debug ascii-client-id** command to display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output.

Examples

The following example shows how to display the client ID in ASCII format in Dynamic Host Configuration Protocol (DHCP) debug output:

```
Router(config)# ip dhcp debug ascii-client-id
```

Related Commands

Command	Description
odap client	Configures ODAP client parameters.

ip dhcp excluded-address

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
ip address pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.

ip dhcp global-options

To enter DHCP global options configuration mode, which is used to configure DHCP-related global configurations, use the **ip dhcp global-options** command in global configuration mode. To remove DHCP-related global configurations, use the **no** form of this command.

ip dhcp global-options

no ip dhcp global-options

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP-related global options are not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You can configure DHCP options that are common for all pools in DHCP global options configuration mode.

Examples

The following example shows how to enter DHCP global options configuration mode:

```
Router(config)# ip dhcp global-options
Router(config-dhcp-global-options)#
```

Related Commands

Command	Description
dns-server (config-dhcp-global-options)	Configures the DNS IP servers that are available to DHCP clients on request.

ip dhcp limit lease

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

ip dhcp limit lease *lease-limit*

no ip dhcp limit lease *lease-limit*

Syntax Description

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

Command Default

There is no lease limit on an interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

Command	Description
show ip dhcp limit lease	Displays the number of times the lease limit threshold has been violated on an interface.

ip dhcp limit lease log

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

ip dhcp limit lease log

no ip dhcp limit lease log

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP lease violation logging is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp limit lease per interface

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

ip dhcp limit lease per interface *lease-limit*

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

Syntax Description

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

Command Default

The number of leases offered is not limited.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dhcp limited-broadcast-address

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

ip dhcp limited-broadcast-address

no ip dhcp limited-broadcast-address

Syntax Description

This command has no arguments or keywords.

Command Default

Default broadcast address: 255.255.255.255 (all ones)

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example configures DHCP to override any network broadcast:

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

Related Commands

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

ip dhcp ping packets

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

ip dhcp ping packets *number*

no ip dhcp ping packets

default ip dhcp ping packets

Syntax Description

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

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.