



## **accounting dhcp through clear ip route**

## accounting (DHCP)

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

**accounting** *server-group-name*

**no accounting** *server-group-name*

### Syntax Description

*server-group-name*

Name of a server group to apply DHCP accounting.

- The server group can have one or more members. The server group is defined in the configuration of the **aaa group server** and **aaa accounting** commands.

### Command Default

DHCP accounting is not enabled by default.

### Command Modes

DHCP pool configuration (dhcp-config)

### Command History

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

### Usage Guidelines

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

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

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

### Command Examples

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

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

### Related Commands

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

Command	Description
<b>show ip dhcp binding</b>	Displays address bindings on the Cisco IOS DHCP server.
<b>show ip dhcp server statistics</b>	Displays Cisco IOS DHCP server statistics.
<b>update arp</b>	Secures the MAC address of the authorized client interface to the DHCP binding.

## address client-id

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

**address** *ip-address* **client-id** *string* [*ascii*]  
**no address** *ip-address*

### Syntax Description

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

### Command Default

IP addresses are not reserved.

### Command Modes

DCHP pool configuration (dhcp-config)

### Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

### Usage Guidelines

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

### 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
<b>address hardware address</b>	Reserves an IP address for a client identified by hardware address.

---

## address hardware-address

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

```
address ip-address hardware-address mac-address [hardware-number ]  
no address ip-address
```

### Syntax Description

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

### Command Default

IP addresses are not reserved.

### Command Modes

DHCP pool configuration (dhcp-config)

### Command History

Release	Modification
12.2(46)SE	This command was introduced.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

### Usage Guidelines

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

### Command Examples

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

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

**Related Commands**

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



# address range

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

**address range** *start-ip end-ip*

**no address range** *start-ip end-ip*

## Syntax Description

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

## Command Default

No DHCP address range is set.

## Command Modes

DHCP pool class configuration (config-dhcp-pool-class)

## Command History

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

## Usage Guidelines

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

**Command Examples**

The following example shows how to set the available address range for class 1 from 10.0.20.1 through 10.0.20.100:

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

**Related Commands**

Command	Description
<b>ip dhcp class</b>	Defines a DHCP class and enters DHCP class configuration mode.

# application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

## application redundancy

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Redundancy configuration (config-red)
----------------------	---------------------------------------

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

<b>Command Examples</b>	The following example shows how to enter redundancy application configuration mode:
-------------------------	---

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

Related Commands	Command	Description
	<b>group (firewall)</b>	Enters redundancy application group configuration mode.

## arp (global)

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

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

### Cisco IOS 12.2(33)SXI Release and Later Releases

```
arp {ip-address | vrf vrf-name | access-list name | clear retry count} hardware-address encap-type
[interface-type] [alias]
no arp {ip-address | vrf vrf-name | access-list name | clear retry count} hardware-address encap-type
[interface-type] [alias]
```

#### Syntax Description

<i>ip-address</i>	IP address in four-part dotted decimal format corresponding to the local data-link address.
<b>vrf</b> <i>vrf-name</i>	Virtual routing and forwarding (VRF) instance. The <i>vrf-name</i> argument is the name of the VRF table.
<b>access-list</b>	Specifies the named access-list.
<i>name</i>	Access-list name.
<b>clear</b>	Clears ARP command parameter.
<b>retry</b>	Specifies the number of retries.
<i>count</i>	Retry attempts. The range is from 1 to 50.
<i>hardware-address</i>	Local data-link address (a 48-bit address).
<i>encap-type</i>	Encapsulation description. The keywords are as follows: <ul style="list-style-type: none"> <li><b>arpa</b> --For Ethernet interfaces.</li> <li><b>sap</b> --For Hewlett Packard interfaces.</li> <li><b>smds</b> --For Switched Multimegabit Data Service (SMDS) interfaces.</li> <li><b>snap</b> --For FDDI and Token Ring interfaces.</li> <li><b>srp-a</b> --Switch Route Processor, side A (SRP-A) interfaces.</li> <li><b>srp-b</b> --Switch Route Processor, side B (SRP-B) interfaces.</li> </ul>

*interface-type*

(Optional) Interface type. For more information, use the question mark (?) online help. The keywords are as follows:

- **ethernet** --IEEE 802.3 interface.
- **loopback** --Loopback interface.
- **null** --No interface.
- **serial** --Serial interface.

**alias**

Responds to ARP requests for the IP address.

#### Command Default

No entries are permanently installed in the ARP cache.

#### Command Modes

Global configuration (config)

#### 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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SXI. The <b>clear</b> and <b>retry</b> keywords were added. The <i>count</i> argument was added.

#### Usage Guidelines

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

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

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

**Command Examples**

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

```
arp 10.31.7.19 0800.0900.1834 arpa
```

**Related Commands**

Command	Description
<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.

## arp (interface)

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

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

### Syntax Description

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

### Command Default

Standard Ethernet-style ARP

### Command Modes

Interface configuration

### Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The <b>probe</b> keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

---

**Usage Guidelines**

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

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

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

---

**Command Examples**

The following example enables Frame Relay services:

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

---

**Related Commands**

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



## arp access-list

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

**arp access-list** *name*

**no arp access-list** *name*

### Syntax Description

<i>name</i>	Name of the access list.
-------------	--------------------------

### Command Default

This command has no default settings.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

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

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

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

<b>permit</b>	Specifies to apply QoS to the flows.
---------------	--------------------------------------

<b>deny</b>	Skips the QoS action that is configured for traffic matching this ACE.
<b>ip</b>	Specifies the IP ARP packets.
<b>any</b>	Specifies any IP ARP packets.
<b>host sender-ip</b>	Specifies the IP address of the host sender.
<i>sender-ip-mask</i>	(Optional) Subnet mask of the host sender.
<b>mac any</b>	Specifies MAC-layer ARP traffic.
<b>no</b>	Deletes an ACE from an ARP ACL.

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

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

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

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

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

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

<b>permit</b>	Specifies packets to forward.
<b>deny</b>	Specifies packets to reject.
<b>ip</b>	Specifies the sender IP address.
<b>any</b>	Specifies any sender IP address.
<b>host</b>	Specifies a single sender host.
<i>sender-ip</i>	IP address of the host sender.
<i>sender-ip-mask</i>	Subnet mask of the host sender.
<b>mac any</b>	Specifies any MAC address.

<b>mac host</b>	Specifies a single sender host MAC address.
<i>sender-mac</i>	MAC address of the host sender.
<i>sender-mac-mask</i>	Subnet mask of the host sender.
<b>log</b>	(Optional) Specifies log on match.
<b>request</b>	Specifies ARP requests.
<b>response</b>	Specifies ARP responses.
<b>any</b>	(Optional) Specifies any target address.
<b>host</b>	(Optional) Specifies a single target host.
<i>target-ip</i>	IP address of the target host.
<i>target-ip-mask</i>	Subnet mask of the target host.
<i>target-mac</i>	MAC address of the target host.
<i>target-mac-mask</i>	Subnet mask of the target host.

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

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

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

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

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

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

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

### Command Examples

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

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

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

```
Router(config)# arp access-list arp_filtering
```

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

**Related Commands**

Command	Description
show arp	Displays information about the ARP table.

## arp authorized

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

**arp authorized**

**no arp authorized**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	No default behavior or values
------------------------	-------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(4)T	This command was introduced.

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

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

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

<b>Command Examples</b>	The following example disables dynamic ARP learning on interface Ethernet 0:
-------------------------	--

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

**Related Commands**

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

## arp log threshold entries

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

**arp log threshold entries** *entry-count*

**no arp log threshold entries**

### Syntax Description

*entry-count*

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

### Command Default

ARP trap is disabled for the interface.

### Command Modes

Interface configuration

### Command History

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

### Usage Guidelines

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

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

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

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

**Command Examples**

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

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

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

```
Router# show logging

Syslog logging: enabled (0 messages dropped, 39 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
  Console logging: disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled,
                    filtering disabled
  Buffer logging: level debugging, 309 messages logged, xml disabled,
                  filtering disabled
  Exception Logging: size (8192 bytes)
  Count and timestamp logging messages: disabled
  Persistent logging: disabled
No active filter modules.
  Trap logging: level informational, 312 message lines logged
Log Buffer (65536 bytes):
Jan 27 18:27:32.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:27:31 PST
Fri Jan 27 2006 to 10:27:32 PST Fri Jan 27 2006, configured from console by console.
Jan 27 18:27:32.431: %SYS-5-CONFIG_I: Configured from console by console
Jan 27 18:27:34.051: %ARP-4-TRAPENTRY: 50 dynamic ARP entries on Ethernet2/1 installed in
the ARP table
```

**Related Commands**

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



## arp packet-priority enable

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

**arp packet-priority enable**  
**no arp packet-priority enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** By default, ARP packet priority is not enabled.

**Command Modes** Interface configuration (config-if)

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

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

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

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

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

**Related Commands**

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

# arp probe interval

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

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

**no arp probe**

## Syntax Description

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

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

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

## Command Examples

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

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

**Related Commands**

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

## arp timeout

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

**arp timeout** *seconds*

**no arp timeout** *seconds*

### Syntax Description

*seconds*

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

### Command Default

14400 seconds (4 hours)

### Command Modes

Interface configuration

### Command History

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

### Usage Guidelines

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

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

**Command Examples**

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

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

**Related Commands**

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

# authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication** command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

**authentication** {*text string* | **md5 key-string** [*0* | *7*] *key* | **md5 key-chain** *key-chain-name*}

**no authentication** {*text string* | **md5 key-string** [*0* | *7*] *key* | **md5 key-chain** *key-chain-name*}

## Syntax Description

<b>text string</b>	Uses clear text authentication.
<b>md5 key-string</b>	Uses MD5 key authentication. The <i>key</i> argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
<b>0</b>	(Optional) Specifies that the text following immediately is not encrypted.
<b>7</b>	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
<b>md5 key-chain</b> <i>key-chain-name</i>	Uses MD5 key-chain authentication.

## Command Default

The key is not encrypted.

## Command Modes

Redundancy application protocol configuration (config-red-app-protcl)

## Command History

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

## Command Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-protcl)# authentication text name1
```

**Related Commands**

Command	Description
<b>application redundancy</b>	Enters redundancy application configuration mode.
<b>group</b>	Enters redundancy application group configuration mode.
<b>name</b>	Configures the redundancy group with a name.
<b>preempt</b>	Enables preemption on the redundancy group.
<b>protocol</b>	Defines a protocol instance in a redundancy group.
<b>timers hellotime</b>	Configures timers for hellotime and holdtime messages for a redundancy group.



## authorization method (DHCP)

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

**authorization method** *method-list-name*

**no authorization method** *method-list-name*

### Syntax Description

*method-list-name*

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

### Command Default

The authorization network default method list is used for authorization.

### Command Modes

DHCP pool configuration (config-dhcp)

### Command History

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

### Usage Guidelines

The method list must be defined during initial authentication setup.

### Command Examples

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

```
Router(config)# aaa authorization network auth1 group radius
```

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

**Related Commands**

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

## authorization shared-password

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

**authorization shared-password** *password*

**no authorization shared-password** *password*

### Syntax Description

*password*

The password configured in the RADIUS user profile.

### Command Default

No password is sent in the RADIUS requests.

### Command Modes

DHCP pool configuration (config-dhcp)

### Command History

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

### Usage Guidelines

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

### Command Examples

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

```
Router(config)# ip dhcp pool pool_common
```

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

**Related Commands**

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

## authorization username (DHCP)

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

**authorization username** *string*

**no authorization username** *string*

### Syntax Description

*string*

A string that RADIUS sends to the DHCP server when downloading an IP address and other configuration information for a client's DHCP responses.

The string must contain the following formatting characters to insert information associated with the DHCP client:

- **%%** --Transmits the percent sign (%) character in the string sent to the RADIUS server
- **%c** --Ethernet address of the DHCP client (chaddr field) in ASCII format
- **%C** --Ethernet address of the DHCP client in hexadecimal format
- **%g** --Gateway address of the DHCP relay agent (giaddr field)
- **%i** --Inner VLAN ID from the DHCP relay information (option 82) in ASCII format
- **%I** --Inner VLAN ID from the DHCP relay information in hexadecimal format
- **%o** --Outer VLAN ID from the DHCP relay information (option 82) in ASCII format
- **%O** --Outer VLAN ID from the DHCP relay information (option 82) in hexadecimal format
- **%p** --Port number from the DHCP relay information (option 82) in ASCII format
- **%P** --Port number from the DHCP relay information (option 82) in hexadecimal format
- **%u** --Circuit ID from the DHCP relay information in ASCII format
- **%U** --Circuit ID from the DHCP relay information in hexadecimal format
- **%r** --Remote ID from the DHCP relay information in ASCII format

- **%R** --Remote ID from the DHCP relay information in hexadecimal format

**Note** The percent (%) is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% character.

### Command Default

No parameters are specified.

### Command Modes

DHCP pool configuration (config-dhcp)

### Command History

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

### Usage Guidelines

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

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

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

For example, if you specify **%C** with the **authorization username** command and the hardware address of the client is aabb.ccdd.eeff, then the DHCP server sends the username as “dhcp-AABBCCDDEEFF” in

ASCII format. If you specify %c with the **authorization username** command, then the DHCP server sends the username as “646863702daabbccddeeff” in hexadecimal format. The server sends 11 bytes of data when the format is hexadecimal and 19 bytes when the format is ASCII.

### Command Examples

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

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

### Related Commands

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

# bootfile

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

**bootfile** *filename*

**no bootfile**

## Syntax Description

*filename*

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

## Command Default

No default behavior or values.

## Command Modes

DHCP pool configuration

## Command History

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

## Command Examples

The following example specifies xllboot as the name of the boot file:

```
bootfile xllboot
```

## Related Commands

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



Command	Description
<b>next-server</b>	Configures the next server in the boot process of a DHCP client.

## class (DHCP)

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

**class** *class-name*

**no class** *class-name*

### Syntax Description

*class-name*

Name of the DHCP class.

### Command Default

No class is associated with the DHCP address pool.

### Command Modes

DHCP pool configuration (dhcp-config)

### Command History

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

### Usage Guidelines

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

### Command Examples

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

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# network 10.0.20.0 255.255.255.0
```

```
Router(dhcp-config)# class class1
Router(config-dhcp-pool-class)# address range 10.0.20.1 10.0.20.100
Router(config-dhcp-pool-class)# exit
Router(dhcp-config)# class class2
Router(config-dhcp-pool-class)# address range 10.0.20.101 10.0.20.200
```

---

**Related Commands**

Command	Description
<b>ip dhcp class</b>	Defines a DHCP class and enters DHCP class configuration mode.

---

# clear arp interface

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

**clear arp interface** *type number*

## Syntax Description

<i>type</i>	Interface type.
<i>number</i>	Interface number.

## Command Default

No default behavior or values.

## Command Modes

Privileged or User EXEC

## Command History

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

## Usage Guidelines

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

**Command Examples**

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

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

# clear arp-cache

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

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

## Syntax Description

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

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	The <b>interface</b> keyword and the <i>type</i> and <i>number</i> arguments were made optional to support refreshing of entries for a single router interface. The <b>vrf</b> keyword, the <i>vrf-name</i> argument, and the <i>ip-address</i> argument were added to support refreshing of entries of a specified address and an optionally specified VRF.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

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

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



#### Note

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

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

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



#### Tip

The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *type* and *number* arguments in the **clear arp-cache interface** command.

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

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

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

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

**Command Examples**

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

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

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

```
Router# clear arp-cache interface ethernet 1/2
```

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

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

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

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

**Related Commands**

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



## clear arp-cache counters ha

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

**clear arp-cache counters ha**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

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

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

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



**Note**

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

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

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

**Related Commands**

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

# clear host

To delete hostname-to-address mapping entries from one or more hostname caches, use the **clear host** command in privileged EXEC mode.

```
clear host [view view-name | vrf vrf-name | all] {hostname | *}
```

## Syntax Description

<b>view</b> <i>view-name</i>	(Optional) The <i>view-name</i> argument specifies the name of the Domain Name System (DNS) view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<b>vrf</b> <i>vrf-name</i>	(Optional) The <i>vrf-name</i> argument specifies the name of the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.
<b>all</b>	(Optional) Specifies that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view.
<i>hostname</i>	Name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache.
*	Specifies that all the hostname-to-address mappings are to be deleted from the specified hostname cache.

## Command Default

No hostname-to-address mapping entries are deleted from any hostname cache.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
12.4(4)T	The <b>vrf</b> keyword, <i>vrf-name</i> argument, and <b>all</b> keyword were added.
12.4(9)T	The <b>view</b> keyword and <i>view-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

This command clears the specified hostname cache entries in running memory, but it does not remove the entries from NVRAM.

Entries can be removed from the hostname caches for a DNS view name, from the hostname caches for a VRF, or from all configured hostname caches. To remove entries from hostname caches for a particular DNS view name, use the **view** keyword and *view-name* argument. To remove entries from the hostname caches for a particular VRF, use the **vrf** keyword and *vrf-name* argument. To remove entries from all configured hostname caches, use the **all** keyword.

To remove entries that provide mapping information for a single hostname, use the *hostname* argument. To remove all entries, use the **\*** keyword.

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.

To define static hostname-to-address mappings in the DNS hostname cache for a DNS view, use the **ip host** command.

### Command Examples

The following example shows how to clear all entries from the hostname cache for the default view in the global address space:

```
Router# clear host all *
```

The following example shows how to clear entries for the hostname www.example.com from the hostname cache for the default view associated with the VPN named vpn101:

```
Router# clear host vrf vpn101 www.example.com
```

The following example shows how to clear all entries from the hostname cache for the view named user2 in the global address space:

```
Router# clear host view user2 *
```

**Related Commands**

Command	Description
<b>ip host</b>	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
<b>show hosts</b>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

# clear ip arp inspection log

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

## clear ip arp inspection log

### Syntax Description

This command has no arguments or keywords.

### 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.

### Command Examples

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

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

### Related Commands

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

# clear ip arp inspection statistics

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

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

## Syntax Description

<b>vlan</b> <i>vlan-range</i>	(Optional) Specifies the VLAN range.
-------------------------------	--------------------------------------

## 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.

## Command Examples

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

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

## Related Commands

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

# clear ip dhcp binding

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

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

## Syntax Description

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

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

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

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



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

### Command Examples

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

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

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

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

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

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

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

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

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

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

### Related Commands

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

# clear ip dhcp conflict

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

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

## Syntax Description

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

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

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

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

### Command Examples

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

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

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

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

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

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

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

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

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

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

### Related Commands

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

# clear ip dhcp limit lease

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

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

## Syntax Description

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

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

## Command Examples

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

```
Router# show ip dhcp limit lease
Interface      Count
Serial0/0.1    5
Serial1        3
Router# clear ip dhcp limit lease
Router# show ip dhcp limit lease
```

## Related Commands

Command	Description
<b>ip dhcp limit lease</b>	Limits the number of leases offered to DHCP clients per interface.

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

# clear ip dhcp server statistics

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

## clear ip dhcp server statistics

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

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

### Usage Guidelines

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

### Command Examples

The following example resets all DHCP counters to zero:

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

### Related Commands

Command	Description
<b>show ip dhcp server statistics</b>	Displays Cisco IOS DHCP server statistics.

# clear ip dhcp snooping binding

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

## clear ip dhcp snooping binding

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command has no default settings.

**Command Modes** Privileged EXEC

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

**Command Examples** This example shows how to clear the DHCP-snooping binding-entry table:

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

# clear ip dhcp snooping database statistics

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

**clear ip dhcp snooping database statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Command Examples

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

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



# clear ip dhcp snooping statistics

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

## clear ip dhcp snooping statistics

**Syntax Description** This command has no arguments or keywords.

**Command Default** This command has no default settings.

**Command Modes** Privileged EXEC

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

**Command Examples** This example shows how to clear the DHCP snooping statistics:

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

# clear ip dhcp subnet

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

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

## Syntax Description

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

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

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

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

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



### Caution

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

**Command Examples**

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

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

The following example clears all leased subnets from all pools:

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

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

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

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

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

**Related Commands**

Command	Description
<b>show ip dhcp pool</b>	Displays information about the DHCP address pools.

## clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in EXEC mode.

```
clear ip nat translation { * | forced | [piggyback-internal | esp | tcp | udp] [inside global-ip  
[ global-port ] local-ip [ local-port ] outside local-ip global-ip] | [inside global-ip local-ip [forced]] |  
[outside local-ip global-ip [forced]] }
```

### Syntax Description

<b>*</b>	Clears all dynamic translations.
<b>forced</b>	(Optional) Forces the clearing of either: <ul style="list-style-type: none"> <li>all dynamic entries, whether or not there are any child translations.</li> <li>a single dynamic half-entry and any existing child translations, whether or not there are any child translations.</li> </ul>
<b>piggyback-internal</b>	(Optional) Clears translations created off of piggyback data.
<b>esp</b>	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
<b>tcp</b>	(Optional) Clears the TCP entries from the translation table.
<b>udp</b>	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.
<b>inside</b>	(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses. If used without the <b>forced</b> keyword, clears only those entries that do not have child translations.
<i>global-ip</i>	(Optional) Global IP address.
<i>global-port</i>	(Optional) Global port.
<i>local-ip</i>	(Optional) Local IP address.
<i>local-port</i>	(Optional) Local port.
<b>outside</b>	(Optional) Clears the outside translations containing the specified <i>local-ip</i> and <i>global-ip</i> addresses. If used without the <b>forced</b> keyword, clears only those entries that do not have child translations.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	The <b>esp</b> keyword was added.
	12.2 (33) XND	The <b>forced</b> keyword was extended to support the removal of a half entry regardless of whether it has any child translations.
	12.4(2)T	The <b>piggyback-internal</b> keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	XE 2.4.2	The <b>forced</b> keyword was extended to support the removal of a half entry regardless of whether it has any child translations.

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

**Command Examples** The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router> show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
udp 10.69.233.209:1220 10.168.1.95:1220 10.69.2.132:53     10.69.2.132:53
tcp 10.69.233.208      10.168.1.94
tcp 10.69.233.209:11012 10.168.1.89:11012 10.69.1.220:23     10.69.1.220:23
tcp 10.69.233.209:1067 10.168.1.95:1067 10.69.1.161:23     10.69.1.161:23
Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
outside 10.69.2.132 53 10.69.2.132 53
Router# show ip nat translations

Pro      Inside global      Inside local      Outside local      Outside global
tcp      10.69.233.208      10.168.1.94
tcp      10.69.233.209:11012 10.168.1.89:11012 10.69.1.220:23     10.69.1.220:23
tcp      10.69.233.209:1067 10.168.1.95:1067 10.69.1.161:23     10.69.1.161:23
Router# clear ip nat translation inside 10.69.233.208 10.168.1.94 forced
Router# show ip nat translations

Pro      Inside global      Inside local      Outside local      Outside global
tcp      10.69.233.209:11012 10.168.1.89:11012 10.69.1.220:23     10.69.1.220:23
tcp      10.69.233.209:1067 10.168.1.95:1067 10.69.1.161:23     10.69.1.161:23
```

**Related Commands**

Command	Description
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Changes the amount of time after which NAT translations time out.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

## clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol ( NHRP) cache, use the **clear ip nhrp** command in EXEC mode.

```
{ clear ip nhrp [dest_ip-address [ dest_mask ]] | [counters {interface if-name if-number | vrf vrf-name }} ] | [shortcut [interface if-name if-number]] }
```

### Syntax Description

<i>dest_ip-address</i>	(Optional) Clears NHRP mapping entries for specified destination IP addresses.
<i>dest_mask</i>	(Optional) Name of the destination network mask.
<b>counters</b>	(Optional) Clears the NHRP counters.
<b>interface</b>	(Optional) Clears NHRP mapping entries for the specified interface.
<i>if-name</i>	(Optional) Interface name. Specifying this arguments removes the specified interface name that all entries learned via this interface from the Next Hop Resolution Protocol ( NHRP) cache.
<i>if-number</i>	(Optional) Interface number. Specifying this arguments removes the specified interface number that all entries learned via this interface from the Next Hop Resolution Protocol ( NHRP) cache.
<b>vrf</b>	(Optional) Deletes entries from the Next Hop Resolution Protocol ( NHRP) cache for the specified VRF.
<i>vrf-name</i>	(Optional) Name of the VRF address-family to which the command is applied.
<b>shortcut</b>	(Optional) Deletes shortcut entries from the Next Hop Resolution Protocol ( NHRP) cache.

### Command Modes

User EXEC Privileged EXEC

### Command History

Release	Modification
11.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was modified. Support was added for the <b>shortcut</b> keyword.

### Usage Guidelines

This command does not clear any static (configured) IP-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache. The **clear ip nhrp shortcut** command clears NHRP cache entries that have associated NHRP routes/nexthop-overrides in the RIB.

### Command Examples

The following example clears all dynamic entries from the NHRP cache for the interface:

```
Router> clear ip nhrp
```

The following example shows how to clear NHRP cache entries that have associated NHRP routes/nexthop-overrides in the RIB:

```
Router> clear ip nhrp shortcut
```

### Related Commands

Command	Description
<b>show ip nhrp</b>	Displays the NHRP cache.



# clear ip route

To delete routes from the IP routing table, use the **clear ip route** command in EXEC mode.

**clear ip route** { *network* [ *mask* ] | \* }

## Syntax Description

<i>network</i>	Network or subnet address to remove.
<i>mask</i>	(Optional) Subnet address to remove.
*	Removes all routing table entries.

## Command Default

All entries are removed.

## Command Modes

EXEC

## Command History

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

## Command Examples

The following example removes a route to network 10.5.0.0 from the IP routing table:

```
Router> clear ip route 10.5.0.0
```