address dhcp through ip arp inspection validate

address range

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

address range *start-ip end-ip*

no address range *start-ip end-ip*

Syntax Description

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

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.

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
ip dhcp class	Defines a DHCP class and enters DHCP class 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

ip-address	IP address in four-part dotted decimal format corresponding to the local data-link address.
vrf *vrf-name*	Virtual routing and forwarding (VRF) instance. The *vrf-name* argument is the name of the VRF table.
access-list	Specifies the named access-list.
name	Access-list name.
clear	Clears ARP command parameter.
retry	Specifies the number of retries.
count	Retry attempts. The range is from 1 to 50.
hardware-address	Local data-link address (a 48-bit address).
encap-type	Encapsulation description. The keywords are as follows: • **arpa** --For Ethernet interfaces. • **sap** --For Hewlett Packard interfaces. • **smds** --For Switched Multimegabit Data Service (SMDS) interfaces. • **snap** --For FDDI and Token Ring interfaces. • **srp-a** --Switch Route Processor, side A (SRP-A) interfaces. • **srp-b** --Switch Route Processor, side B (SRP-B) interfaces.

interface-type	(Optional) Interface type. 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 **clear** and **retry** keywords were added. The *count* 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.

Examples

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

```
arp 10.31.7.19 0800.0900.1834 arpa
```

Related Commands

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

arp (interface)

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

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

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

Syntax Description

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

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 **probe** keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

Examples

The following example enables Frame Relay services:

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

Related Commands

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

arp access-list

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

arp access-list *name*

no arp access-list *name*

Syntax Description

name	Name of the access list.

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**

permit	Specifies to apply QoS to the flows.
deny	Skips the QoS action that is configured for traffic matching this ACE.
ip	Specifies the IP ARP packets.
any	Specifies any IP ARP packets.

host *sender-ip*	Specifies the IP address of the host sender.
sender-ip-mask	(Optional) Subnet mask of the host sender.
mac any	Specifies MAC-layer ARP traffic.
no	Deletes an ACE from an ARP ACL.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

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

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

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

Related Commands

Command	Description
show arp	Displays information about the ARP table.

arp 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 ininterface 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
```

Examples

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

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

Related Commands

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

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.

Examples

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

```
bootfile xllboot
```

Related Commands

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

class (DHCP)

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

class *class-name*

no class *class-name*

Syntax Description

class-name	Name of the DHCP class.

Command Default

No class is associated with the DHCP address pool.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear arp interface

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

clear arp interface *type number*

Syntax Description

type	Interface type.
number	Interface number.

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.

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

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

Command Default

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

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 hours.

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

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

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

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

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

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

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

Examples

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

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

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

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

clear 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.

Examples

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

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

Related Commands

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

clear ip arp inspection statistics

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

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

Syntax Description

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

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.

Examples

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

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

Related Commands

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

clear ip dhcp binding

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip dhcp conflict

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The server detects conflicts using a ping 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.

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip dhcp server statistics

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

clear ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example resets all DHCP counters to zero:

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

Related Commands

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

clear ip dhcp snooping binding

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

clear ip dhcp snooping binding

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear ip dhcp snooping database statistics

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

clear ip dhcp snooping database statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

clear ip dhcp snooping statistics

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

clear ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to clear the DHCP snooping statistics:

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

clear ip route

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

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

Syntax Description

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

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.

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
```

client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** command in DHCP pool configuration mode. To delete the client identifier, use the **no** form of this command.

client-identifier *unique-identifier*

no client-identifier

Syntax Description

unique-identifier	The distinct identification of the client in 7- or 27-byte dotted hexadecimal notation. See the "Usage Guidelines" section for more information.

Command Default

No client identifier is specified.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Usage Guidelines

This command is valid for manual bindings only. DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. You can specify the unique identifier for the client in either of the following ways:

- A 7-byte dotted hexadecimal notation. For example, 01b7.0813.8811.66, where 01 represents the Ethernet media type and the remaining bytes represent the MAC address of the DHCP client.
- A 27-byte dotted hexadecimal notation. For example, 7665.6e64.6f72.2d30.3032.342e.3937.6230.2e33.3734.312d.4661.302f.31. The equivalent ASCII string for this hexadecimal value is vendor-0024.97b0.3741-fa0/1, where vendor represents the vendor, 0024.97b0.3741 represents the MAC address of the source interface, and fa0/1 represents the source interface of the DHCP client.

For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, *Assigned Numbers*.

You can determine the client identifier by using the **debug ip dhcp server packet** command.

Examples

The following example specifies the client identifier for MAC address 01b7.0813.8811.66 in dotted hexadecimal notation:

```
Device(dhcp-config)# client-identifier 01b7.0813.8811.66
```

Related Commands

Command	Description
hardware-address	Specifies the hardware address of a BOOTP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

client-name

To specify the name of a Dynamic Host Configuration Protocol (DHCP) client, use the **client-name** command in DHCP pool configuration mode. To remove the client name, use the **no** form of this command.

client-name *name*

no client-name

Syntax Description

name	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name abc should not be specified as abc.cisco.com.

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.

Usage Guidelines

The client name should not include the domain name.

Examples

The following example specifies a string client1 that will be the name of the client:

```
client-name client1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.

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

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2 ... address8*]

no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

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.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the default router:

```
default-router 10.12.1.99
```

Related Commands

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

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2 ... address8*]

no dns-server

Syntax Description

address	The IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
dns-server 10.12.1.99
```

Related Commands

Command	Description
domain-name (DHCP)	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

domain name

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain name** command in DNS view configuration mode. To remove the specification of the default domain name for a DNS view, use the **no** form of this command.

domain name *domain-name*

no domain name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DNS view configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command configures the default domain name used to complete unqualified hostnames in DNS queries handled using the DNS view.

Note The **domain list** and **domain name** commands are similar, except that the **domain list** command can be used to define a list of domain names for the view, each to be tried in turn. If DNS lookup is enabled for the DNS view but the domain search list (specified using the **domain list** command) is empty, the default domain name (specified by using the **domain name** command) is used instead. If the domain search list is not empty, the default domain name is not used.

To display the default domain name configured for a DNS view, use the **show hosts** command or the **show ip dns view** command.

Examples

The following example shows how to define example.com as the default domain name for the DNS view named user3 that is associated with the VRF vpn32:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# domain name example.com
```

Related Commands

Command	Description
domain list	Defines the ordered list of default domain names to use to complete unqualified hostnames in internally generated DNS queries handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

hardware-address

To specify the hardware address of a BOOTP client, use the **hardware-address** command in DHCP pool configuration mode. To remove the hardware address, use the no form of this command.

hardware-address *hardware-address* [*protocol-type*| *hardware-number*]

no hardware-address

Syntax Description

hardware-address	MAC address of the client.
protocol-type	(Optional) Protocol type. The valid entries are: • **ethernet** • **ieee802** If no protocol type is specified, the default is Ethernet.
hardware-number	(Optional) ARP hardware specified in an online database at http://www.iana.org/assignments/arp-parameters. The valid range is from 0 to 255. See the table below for valid entries.

Command Default

Only the hardware address is enabled.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

This command is valid for manual bindings only.

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

Table 1: ARP Hardware Numbers and Types

Hardware Number	Hardware Type
1	Ethernet
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25
4	ProNET Token Ring
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM) (RFC2225)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)
22	MIL-STD-188-220
23	Metricom

Hardware Number	Hardware Type
24	IEEE 1394.1995
25	MAPOS and Common Air Interface (CAI)
26	Twinaxial
27	EUI-64
28	HIPARP
29	IP and ARP over ISO 7816-3
30	ARPSec
31	IPsec tunnel (RFC3456)
32	InfiniBand (RFC-ietf-ipoib-ip-over-infiniband-09.txt)
33	TIA-102 Project

Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
hardware-address b708.1388.f166 ieee802
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a DHCP client in dotted hexadecimal notation.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host**command in DHCP pool configuration mode. To remove the IP address of the client, use the no form of this command.

host *address* [*mask*| /*prefix-length*]

no host

Syntax Description

address	Specifies the IP address of the client.
mask	(Optional) Specifies the network mask of the client.
/ *prefix-length*	(Optional) Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Command Default

The natural mask is used.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

If the mask and prefix length are unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used. This command is valid for manual bindings only.

There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

Examples

The following example specifies 10.12.1.99 as the IP address of the client and 255.255.248.0 as the subnet mask:

```
host 10.12.1.99 255.255.248.0
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
hardware-address	Specifies the hardware address of a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

import all

To import Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP server database, use the **import all** command in DHCP pool configuration mode. To disable this feature, use the **no** form of this command.

import all

no import all

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **no import all** command is used, the DHCP server deletes all "imported" option parameters that were added to the specified pool in the server database. Manually configured DHCP option parameters override imported DHCP option parameters.

Imported option parameters are not part of the router configuration and are not saved in NVRAM.

Examples

The following example allows the importing of all DHCP options for a pool named pool1:

```
ip dhcp pool pool1
 network 172.16.0.0 /16
 import all
```

Related Commands

Command	Description
ip dhcp database	Configures a DHCP server to save automatic bindings on a remote host called a database agent.

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

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The **vrf** keyword and *vrf-name* argument were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).

- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb**command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autoclassify source
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp**command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the router. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id**keyword and *interface-type number*argument were added.
12.2(3)	This command was modified. The **hostname**keyword and *hostname*argument were added. The behavior of the **client-id** *interface-type number*option changed. See the “Usage Guidelines” section for details.

Release	Modification
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelin

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type*is the Ethernet interface where the command is configured and *interface-type number*is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 2: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
```

```
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname def
```

Related Commands

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

ip 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.