ARP Commands

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*]

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

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.
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. The keywords are as follows: • **ethernet**—IEEE 802.3 interface. • **loopback**—Loopback interface. • **null**—No interface. • **serial**—Serial interface. • **alias**—Cisco IOS software responds to ARP requests as if it were the interface of the specified address.

Defaults   No entries are permanently installed in the ARP cache.

Command Modes   Global configuration

Command History

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

Usage Guidelines   The Cisco IOS software 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.

Defaults 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.

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** EXEC 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** privileged EXEC 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.

Defaults

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 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

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values

Command Modes   Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines   The **arp authorized** 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.

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.

Examples   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
arp (global)	Adds a permanent entry in the ARP cache.
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

Cisco IOS IP Addressing Services Command Reference

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.

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

Cisco IOS IP Addressing Services Command Reference

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.

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
interface	Configures an interface and enters interface configuration mode.
ip address	Sets a primary or secondary IP address for an interface.
shutdown (interface)	Disables an interface.

arp probe interval

To control the the probing 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

seconds	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.
count *count-number*	Number of probe retries. If no response, the peer has logged off. The range is from 1 to 60.

Defaults   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.

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
arp (interface)	Controls the interface-specific handling of IP address resolution.
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.

Cisco IOS IP Addressing Services Command Reference ■

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.

Defaults   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.

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

No default behavior or values.

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(23)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 minutes.

Cisco IOS IP Addressing Services Command Reference

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 ethernet1/2
```

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 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]).

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

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

Related Commands

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

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.

Defaults 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
```

Cisco IOS IP Addressing Services Command Reference

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.

Defaults   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.	

Defaults   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.

Cisco IOS IP Addressing Services Command Reference ■

ip arp entry learn

To specify the maximum number of learned Address Resolution Protocol (ARP) entries, use the **ip arp entry learn** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip arp entry learn *max-limit*

no ip arp entry learn *max-limit*

Syntax Description		
max-limit	The maximum number of learned ARP entries; valid values are from 1 to 512000.	

Command Default

No maximum number of learned ARP entries is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD3	This command was introduced to support the Cisco 7600 router.

Usage Guidelines

The **ip arp entry learn** command is available on the Cisco 7600 series routers, which can support a maximum limit of learned ARP entries of 256,000. If a memory card is installed on the router the maximum limit is extended to 512,000.

When the number of ARP entries that can be created by the system is not limited, memory exhaustion can cause system instability. The **ip arp entry learn** command overcomes this problem by defining a maximum number of learned ARP entries.

The limit is not enforced on nonlearned entries. Upon reaching the learn ARP entry threshold limit, or 80 percent of the configured maximum limit, the system will generate a syslog message with a priority set to Level 3 (LOG_NOTICE). Upon reaching the configured maximum limit, the system starts discarding newly learned ARP entries and generates a syslog message. The priority will be set to Level 3 (LOG_NOTICE). The system administrator will have to take appropriate action.

A syslog message is also generated when the number of learned ARP entries in the ARP table decreases from the maximum configured limit to the permit threshold limit, or 95 percent of the maximum configured limit to notify the system administrator that the ARP table is back to normal operation.

The default behavior of the system is not to enforce a maximum limit of learned ARP entries on the system.

When a user tries to configure a maximum limit value for the number of ARP entries that is lower than the current number of ARP entries in the system, the configuration will be rejected with an error message.

The following example configures a maximum limit of the number of learned ARP entries of 512,000:

```
Router# configure terminal
Router(config)# ip arp entry learn 512000
```

Related Commands	Command	Description
	show arp summary	Displays the total number of ARP table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router.

ip arp gratuitous

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

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

no ip arp gratuitous

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

Command Default   Gratuitous ARP control is enabled.

Command Modes   Global configuration (config)

Command History

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

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

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

Related Commands

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

ip arp incomplete

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

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

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

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

Command Modes Global configuration (config)

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

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

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

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

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

Cisco IOS IP Addressing Services Command Reference ■

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.	

Defaults 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.

Defaults

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).	

Defaults   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.

Defaults   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.

Defaults   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
```

Cisco IOS IP Addressing Services Command Reference

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

ip arp inspection vlan

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

>**ip arp inspection vlan** *vlan-range*

>**no ip arp inspection vlan** *vlan-range*

Syntax Description

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

Defaults   ARP inspection is disabled on all VLANs.

Command Modes   Global configuration

Command History

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

Usage Guidelines   For *vlan-range*, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if the VLAN has not been created or is a private VLAN.

Examples   This example shows how to enable DAI on VLAN 1:

```
Router(config)# ip arp inspection vlan 1
```

Related Commands

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

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command in global configuration mode. To disable this logging control, use the **no** form of this command.

> **ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**permit** | **all** | **none**}}

> **no ip arp inspection vlan** *vlan-range* **logging** {**acl-match** | **dhcp-bindings**}

Syntax Description

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

Defaults   All denied or dropped packets are logged.

Command Modes   Global configuration

Command History

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

Usage Guidelines   By default, the **matchlog** keyword is not available on the ACEs. When you enter the **matchlog** keyword, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny.

- **dhcp-bindings**—Logging on DHCP bindings is reset to log on deny.

Examples   This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs:

```
Router(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

Related Commands

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

ip arp proxy disable

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

ip arp proxy disable

no ip arp proxy disable

Syntax Description   This command has no arguments or keywords.

Command Default   Proxy ARP is enabled.

Command Modes   Global configuration

Command History

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

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

Examples   The following example disables proxy ARP:

```
ip arp proxy disable
```

The following example enables proxy ARP:

```
no ip arp proxy disable
```

Related Commands

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

ip gratuitous-arps

To enable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in an address pool if the transmission has been disabled, use the **ip gratuitous-arps** command in global configuration mode. To disable the transmission, use the **no** form of this command.

> **ip gratuitous-arps** [**non-local**]

> **no ip gratuitous-arps**

Syntax Description		
non-local		(Optional) Sends gratuitous ARP messages if a client receives an IP address from a non-local address pool. Gratuitous ARP messages for locally originated peer addresses are not sent by default.

Command Default   Gratuitous ARP messages are not sent out when the client receives the address from the local address pool.

Command Modes   Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2T	The **non-local** keyword was added and the default behavior of the command changed.
12.4(2)T	The name of this command was changed from **no ip gratuitous-arps** to **ip gratuitous-arps**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines   A Cisco router will send out a gratuitous ARP message out of all interfaces when a client connects and negotiates an address over a PPP connection. However, by default, gratuitous ARP messages are not sent out when the client receives the address from the local address pool. The **ip gratuitous-arps non-local** command option is the default form and is not saved in the running configuration.

Cisco 10000 Series Router

To maximize the performance of the router, disable gratuitous ARP requests using the **no ip gratuitous-arps** command.

Examples   The following example enables the sending of gratuitous ARP messages if the transmission has been disabled:

```
ip gratuitous-arps
```

Cisco IOS IP Addressing Services Command Reference ■

ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description   This command has no arguments or keywords.

Defaults   This command is not enabled by default.

Command Modes   Interface configuration

Command History

Release	Modification
12.1(5c)EX	This command was introduced on the Catalyst 6500 series switches.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E on the Catalyst 6500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.

Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

Examples   The following example shows how to enable the local proxy ARP feature:

```
ip local-proxy-arp
```

ip proxy-arp

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

ip proxy-arp

no ip proxy-arp

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Interface configuration

Command History

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

Usage Guidelines   The **ip arp proxy disable** command overrides any proxy ARP interface configuration.

Examples   The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
 ip proxy-arp
```

Related Commands

Command	Description
ip arp proxy disable	Globally disables proxy ARP.

ip sticky-arp (global configuration)

To enable sticky ARP, use the **ip sticky-arp** command in global configuration mode. To disable sticky ARP, use the **no** form of this command.

ip sticky-arp

no ip sticky-arp

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Global configuration

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(18)SXF	This command was changed to support all Layer 3 interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines   In releases prior to Release 12.2(18)SXF, sticky ARP was supported on PVLAN interfaces only.

You can enter the **ip sticky-arp (interface configuration)** command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

Examples   This example shows how to enable sticky ARP:

```
Router(config) ip sticky-arp
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
```

Related Commands	Command	Description
	arp	Enables ARP entries for static routing over the SMDS network.
	ip sticky-arp (interface configuration)	Enables sticky ARP on an interface.
	show arp	Displays the ARP table.

ip sticky-arp (interface configuration)

To enable sticky ARP on an interface, use the **ip sticky-arp** command in interface configuration mode. To disable sticky ARP on an interface, use the **no** form of this command.

ip sticky-arp [**ignore**]

no ip sticky-arp [**ignore**]

Syntax Description

ignore	(Optional) Overwrites the **ip sticky-arp** (global configuration) command.

Defaults   This command has no default settings.

Command Modes   Interface configuration

Command History

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

Usage Guidelines   You can enter this command on any Layer 3 interface.

You can enter the **ip sticky-arp ignore** command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.

Examples   This example shows how to enable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp ignore
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (global configuration)	Enables sticky ARP.
show arp	Displays the ARP table.

logging server-arp

To enable the sending of Address Resolution Protocol (ARP) requests for syslog server address during system initialization bootup, use the **logging server-arp** command in global configuration mode. To disable the sending of ARP requests for syslog server addresses, use the **no** form of this command.

> **logging server-arp**

> **no logging server-arp**

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default.

Command Modes   Global configuration.

Command History

Release	Modification
12.3	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(5)B	This command was integrated into Cisco IOS Release 12.3(5)B.

Usage Guidelines   The **logging server-arp** global configuration command allows the sending of ARP requests for syslog server addresses during system initialization bootup.

When this CLI command is configured and saved to the startup configuration file, the system will send an ARP request for remote syslog server address before sending out the first syslog message.

The command should only be used when the remote syslog server is in the same subnet as the system router sending the ARP request.

> **Note**   Use this command even if a static ARP has been configured with the remote syslog server address.

Examples   The following example shows how to enable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# logging server-arp
Router(config)# exit
```

The following example shows how to disable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# no logging server-arp
Router(config)# exit
```

Related Commands	Command	Description
	arp (global)	Adds a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode.

no ip gratuitous-arps

To disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool, use the **no ip gratuitous-arps** command in global configuration mode.

no ip gratuitous-arps

Syntax Description   This command has no keywords or arguments.

Defaults   Disabled

Command Modes   Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines   A Cisco router will send out a gratuitous ARP message when a client connects and negotiates an address over a PPP connection. This transmission occurs even when the client receives the address from a local address pool.

Examples   The following example disables gratuitous arp messages from being sent:

```
no ip gratuitous-arps
```

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** command in user EXEC or privileged EXEC mode.

> **show arp** [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]]
> [**detail**]

Syntax Description		
vrf *vrf-name*	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the *vrf-name* argument.	
	If this option is specified, it can be followed by any valid combination of the *arp-mode*, *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.	
arp-mode	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords:	
	• **alias**—Displays only alias ARP entries. An alias ARP entry is a statically configured (permanent) ARP table entry that is associated with a local IP address. This type of entry can be configured or removed using the **arp** (global) command with the **alias** keyword.	
	• **dynamic**—Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host.	
	• **incomplete**—Displays only incomplete ARP entries. An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host.	
	• **interface**—Displaysonly interface ARP entries. An interface ARP entry contains a local IP address and is derived from an interface.	
	• **static**—Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP entry that is associated with an external host. This type of entry can be configured or removed using the **arp** (global) command.	
	Note If this option is specified, it can be followed by any valid combination of the *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.	
ip-address [*mask*]	(Optional) Displays the entries associated with a specific host or network.	
	Note If this option is specified, it can be followed by any valid combination of the *interface-type* and *interface-number* arguments and the **detail** keyword.	
interface-type interface-number	(Optional) Displays the specified entries that are also associated with this router interface.	
	Note If this option is specified, it can be followed by the **detail** keyword.	
detail	(Optional) Displays the specified entries with mode-specific details and information about subblocks (if any).	

Command Modes   User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
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 the 12.2 SX release.
12.4(11)T	The **vrf** keyword and *vrf-name* argument were added to limit the display to entries under a specific VRF.
	The **alias**, **dynamic**, **incomplete**, **interface**, and **static** keywords were added to limit the display to entries in a specific ARP mode.
	The *ip-address* and *mask* arguments were added to limit the display to entries for a specific host or network.
	The *interface-type* and *interface-number* arguments were added to limit the display to entries for a specific interface.
	The **detail** keyword was added to display additional details about the entries.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines   To display all entries in the ARP cache, use this command without any arguments or keywords.

Entry Selection Options

You can to limit the scope of the command output by applying various combinations of the following ARP entry selection criteria:

- Entries under a specific VRF

- Entries in a specific ARP mode

- Entries for a specific host or entries for a specific network

- Entries associated with a specific router interface

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 *interface-type* and *interface-number* arguments in the **show arp** command.

Detailed Output Format

To include additional details about each ARP entry displayed, use this command with the **detail** keyword. When this display option is used, the following additional information is included:

- Mode-specific details (such as entry update time)

- Subblocks (if any)

ARP Adjacency Notification

If Cisco Express Forwarding (CEF) is enabled on the router, the router maintains forwarding information (outbound interface and MAC header rewrite) for adjacent nodes. A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). CEF stores the forwarding information in an adjacency database so that Layer 2 addressing information can be inserted into link-layer headers attached to the ARP packets.

- To verify that IPv4 CEF is running, use the **show ip cef** command.

- To verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct, use the **show adjacency** command.

The ARP table information is one of the sources for CEF adjacency. Whenever the ARP subsystem attaches an ARP table entry to an outbound interface with a valid hardware address, the subsystem issues an internal "ARP adjacency" notification. The notification causes an ARP background process to synchronize that ARP entry with CEF adjacency via the adjacency database. If the synchronization succeeds, IP ARP adjacency is said to be "installed"; if the synchronization fails, IP ARP adjacency is said to have been "withdrawn."

Note Attachment to an outbound interface occurs only for ARP entries in the following modes: alias, dynamic, static, Application Simple, and Application Timer.

To display detailed information about any ARP adjacency notification that may have occurred, use the **show arp** command with the **detail** keyword. You can use this information to supplement the information available through ARP/CEF adjacency debug trace. To enable debug trace for ARP/CEF adjacency interactions, use the **debug arp** command with the **adjacency** keyword.

ARP Cache Administration

To refresh all entries for the specified interface (or all interfaces) or to refresh all entries of the specified address (or all addresses) in the specified VRF table (or in the global VRF table), use the **clear arp-cache** command.

To enable debugging output for ARP transactions, use the **debug arp** command.

Examples The following is sample output from the **show arp** command with no optional keywords or arguments specified:

```
Router# show arp

Protocol    Address          Age (min)   Hardware Addr    Type    Interface

Internet    192.0.2.112      120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk   4028.5          29          0000.0c01.0e56   SNAP    Ethernet2
Internet    192.0.2.114      105         0000.a710.859b   ARPA    Ethernet3
AppleTalk   4028.9          –           0000.0c02.a03c   SNAP    Ethernet2
Internet    192.0.2.121      42          0000.a710.68cd   ARPA    Ethernet3
Internet    192.0.2.9        –           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk   4036.9          –           0000.3080.6fd4   SNAP    TokenRing0
Internet    192.0.2.9        –           0000.0c01.7bbd   SNAP    Fddi0
```

Table 8 describes the fields shown in the display.

Table 8   show arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • 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—For Switch Route Processor, side A (SRP-A) interfaces. • SRP-B—For Switch Route Processor, side B (SRP-B) interfaces.
Interface	Indicates the interface associated with this network address.

When this command is used to display dynamic ARP entries, the display information includes the time of the last update and the amount of time before the next scheduled refresh is to occur. The following is sample output from the **show arp** command for the dynamic ARP entry at network address 192.0.2.1:

```
Router# show arp 192.0.2.1 detail

ARP entry for 192.0.2.1, link type IP.
  Alias, last updated 13323 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is complete, attached to GigabitEthernet1/1.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.1 on GigabitEthernet1/1) was installed.
```

When this command is used to display floating static ARP entries, the display information includes the associated interface, if any. The following is sample output from the **show arp** command for the floating static ARP entry at network address 192.0.2.2 whose intended interface is down:

```
Router# show arp 192.0.2.2 detail

ARP entry for 192.0.2.2, link type IP.
  Alias, last updated 13327 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
```

```
    * Static ARP Subblock
      Floating entry.
      Entry is incomplete.
    * IP ARP Adjacency
      Adjacency (for 192.0.2.2 on GigabitEthernet1/1) was withdrawn.
```

The following is sample detailed output from the **show arp** command for the Application Alias ARP entry at network address 192.0.2.3:

```
Router# show arp 192.0.2.3 detail

ARP entry for 192.0.2.3, link type IP.
  Application Alias, via Ethernet2/2, last updated 0 minute ago.
  Created by "HSRP".
  Encap type is ARPA, hardware address is 0000.0c07.ac02, 6 bytes long.
  ARP subblocks:
  * Application Alias ARP Subblock
  * HSRP
    ARP Application entry for application HSRP.
```

The following is sample detailed output from the **show arp** command for all dynamic ARP entries:

```
Router# show arp dynamic detail

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1, last updated 0 minute ago.
  Encap type is ARPA, hardware address is 0000.0000.0014, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 0 minute and 1 second.
    It has 1 chance to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
```

Related Commands	Command	Description
	arp (global)	Configures a permanent entry in the ARP cache.
	clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
	debug arp	Enables debugging output for ARP packet transactions.
	show adjacency	Verifies that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.
	show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
	show arp ha	Displays the ARP HA status and statistics.
	show arp summary	Displays the number of the ARP table entries of each mode.
	show interfaces	Displays statistics for all interfaces configured on the router or access server.
	show ip cef	Display entries in the FIB or to display a summary of the FIB.

show arp application

To display Address Resolution Protocol (ARP) table information for a specific ARP application or for all applications supported by ARP and running on registered clients, use the **show arp application** command in user EXEC or privileged EXEC mode.

show arp application [*application-id*] [**detail**]

Syntax Description		
application-id	(Optional) Displays ARP table information for a specific ARP application. The range is from 200 to 4294967295. If no ID is specified, ARP table information is displayed for all supported ARP applications running on registered clients.
detail	(Optional) Includes detailed information about subblocks for ARP table information displayed (for the specified application or for all applications supported by ARP and running on registered clients).

Command Modes   User EXEC
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   To display ARP table information about all supported ARP applications running on registered clients, use this command without any arguments or keywords.

Entry Selection Options

To display ARP table information about a single ARP application running on a registered client, use this command with the *application-ID* argument.

Detailed Output Format

To display the specified ARP table information along with detailed information about any subblocks, use this command with the **detail** keyword. The additional details consist of the following information:

- IP address or network
- ARP table entry type (dynamic, interface, static, or alias) or ARP application mode (Simple Application or Application Alias)
- Associated interface
- Brief description of the subblock data

Cisco IOS IP Addressing Services Command Reference ■

Examples

The following is sample output from the **show arp application** command:

```
Router# show arp application

Number of clients registered: 7

Application      ID      Num of Subblocks
ARP Backup       200     1
IP SIP           201     0
LEC              202     0
DHCPD            203     0
IP Mobility      204     0
HSRP             209     1
IP ARP Adjacency 212     2
```

The following is sample detailed output from the **show arp application detail** command:

```
Router# show arp application detail

Number of clients registered: 7

Application      ID      Num of Subblocks
ARP Backup       200     1

ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    Backup for Interface on Ethernet2/2

Application      ID      Num of Subblocks
IP SIP           201     0

Application      ID      Num of Subblocks
LEC              202     0

Application      ID      Num of Subblocks
DHCPD            203     0

Application      ID      Num of Subblocks
IP Mobility      204     0

Application      ID      Num of Subblocks
HSRP             209     1

ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    ARP Application entry for application HSRP.

Application      ID      Num of Subblocks
IP ARP Adjacency 212     2

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
ARP entry for 192.0.2.2, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.2 on Ethernet2/1) was installed.
```

Table 9 describes the significant fields shown in the display.

Table 9 *show arp application Field Descriptions*

Field	Description
Application	ARP application name
ID	ARP application ID number
Num of Subblocks	Number of subblocks attached

Related Commands

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp ha

To display the status and statistics of Address Resolution Protocol (ARP) high availability (HA), use the **show arp ha** command in user EXEC or privileged EXEC mode.

show arp ha

Syntax Description	This command has no arguments or keywords.

Command Modes	User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines   Use this command to display the ARP HA status and statistics.

HA-Capable Platforms

This command is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

ARP HA Statistics

The ARP HA process collects one set of statistics for the active RP (described in Table 10) and a different set of statistics for the standby RP (described in Table 11). These statistics can be used to track the RP state transitions when debugging ARP HA issues.

The output from this command depends on the current and most recent states of the RP:

- For the active RP that has been the active RP since the last time the router was rebooted, this command displays the HA statistics for the active RP.

- For the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred, this command displays the HA statistics for the active RP plus the HA statistics collected when the RP was a standby RP.

- For a standby RP, this command displays the HA statistics for a standby RP.

Examples   The following is sample output from the **show arp ha** command on the active RP that has been the active RP since the last time the router was rebooted. ARP HA statistics are displayed for the active state only.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  2 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  806 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
```

The following is sample output from the **show arp ha** command on the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred. ARP HA statistics are displayed for the active state and also for the previous standby state.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP).
  1 ARP entry in the synchronization queue.
  1 ARP entry waiting to be synchronized.
  No synchronization packet sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.

Statistics collected when ARP HA in standby state:
  No ARP entry in the backup table.
  808 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  2 ARP entries restored before timer.
  No ARP entry restored on timer.
  No ARP entry purged since interface is down.
  No ARP entry purged on timer.
```

The following is sample output from the **show arp ha** command on the standby RP. ARP HA statistics are displayed for the standby state only.

```
Router# show arp ha

ARP HA in standby state (ARP_HA_ST_S_UP).
  2 ARP entries in the backup table.
  806 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

Table 10 describes the significant fields shown in the display collected for an active RP.

Table 10   show arp ha Field Descriptions for Statistics Collected for an Active RP

Field	Description
ARP HA in active state	The current state that the event-driven state machine contains for the active RP: • ARP_HA_ST_A_UP_SYNC—Active state in which the active RP sends entries from the synchronization queue to the standby RP. The active RP transitions into this state when the number of entries to be synchronized reaches a threshold or when the synchronization timer expires, whichever occurs first. • ARP_HA_ST_A_UP—Active state in which the active RP does not send entries to the standby RP. The active RP transitions into this state either because the standby RP has not come up yet or because a previous synchronization has failed. • ARP_HA_ST_A_BULK—Transient state in which the active RP waits for the standby RP to signal that it has finished processing of the entries sent by the bulk-synchronization operation. • ARP_HA_ST_A_SSO—Transient state in which the new active RP waits for the signal to be fully operational.
ARP entries in the synchronization queue	Number of ARP entries that are queued to be synchronized or have already been synchronized to the standby RP. **Note** Entries that have already been synchronized are kept in the synchronization queue in case the standby RP crashes. After the standby RP reboots, the entire queue (including entries that were already synchronized to the standby RP before the crash) must be bulk-synchronized to the standby RP.
ARP entries waiting to be synchronized	Number of ARP entries that are queued to be synchronized to the standby RP.
synchronization packets sent	Number of synchronization packets that have been sent to the standby RP.
error in allocating synchronization packets	Number of errors that occurred while synchronization packets were being allocated.
error in sending synchronization packets.	Number of errors that occurred while synchronization packets were being sent to the standby RP.
error in encoding interface names	Number of errors that occurred while interface names were being encoded.

Table 11 describes the significant fields shown in the display collected for a standby RP or for an active RP that was previously in the active state.

Table 11   show arp ha Field Descriptions for Statistics Collected for a Standby RP

Field	Description
ARP HA in standby state	The current state that the event-driven state machine contains for the standby RP: • ARP_HA_ST_S_BULK—Transient state in which the standby RP processes the entries sent by the bulk-synchronization operation. After the active RP signals that it has finished sending entries, the standby RP transitions into the ARP_HA_ST_S_UP state and then signals back to the active RP that it has finished processing the entries sent by the bulk-synchronization operation. • ARP_HA_ST_S_UP—Active state in which the standby RP processes the incremental ARP synchronization entries from the active RP. When the switchover occurs, the standby RP transitions to the ARP_HA_ST_A_SSO state.
ARP entries in the backup table	Number of ARP entries contained in the backup ARP table.
synchronization packets processed	Number of synchronization packets that were processed.
synchronization packet dropped in invalid state	Number of synchronization packets that were dropped due to an invalid state.
error in decoding interface names	Number of errors that occurred in decoding interface names.
ARP entries restored before timer	Number of ARP entries that the new active RP restored prior to expiration of the "flush" timer.
ARP entry restored on timer	Number of ARP entries that the new active RP restored upon expiration of the "flush" timer.
ARP entry purged since interface is down	Number of ARP entries that the new active RP purged because the interface went down.
ARP entry purged on timer	Number of ARP entries that the new active RP purged upon expiration of the "flush" timer.

Related Commands

Command	Description
clear arp-cache counters ha	Resets the ARP HA statistics.
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp summary

To display the total number of Address Resolution Protocol (ARP) table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router, use the **show arp summary** command in user EXEC or privileged EXEC mode.

> **show arp summary**

Syntax Description   This command has no arguments or keywords.

Command Modes   User EXEC
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.
12.2(33)SRD3	This command was modified. Support was added for the Cisco 7600 router.

Usage Guidelines   Use this command to display high-level statistics about the ARP table entries:

- Total number of ARP table entries
- Number of ARP table entries for each ARP mode
- Number of ARP table entries for each router interface

A maximum limit for learned ARP entries can be configured on the Cisco 7600 platform in Cisco IOS Release 12.2(33)SRD3. This is subject to memory constraints. The 7600 can support a maximum limit of 256,000 learned ARP entries, and if a memory card is installed on the router the maximum limit is extended to 512,000.

Examples   The following is sample output from the **show arp summary** command:

> **Note**   In this example the maximum limit for the number of learned ARP entries has not been configured.

```
Router# show arp summary

Total number of entries in the ARP table: 10.
Total number of Dynamic ARP entries: 4.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 4.
Total number of Static ARP entries: 2.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
```

```
Interface Entry Count
Ethernet3/2 1
```

The following is sample output from the **show arp summary** command on a Cisco 7600 router for
Cisco IOS Release 12.2(33)SRD3, after a maximum limit is set for the number of learned ARP entries:

```
Router> enable
Router# configure terminal
Router(config)# ip arp entry learn 512000
Router(config)# exit
Router# show arp summary

Total number of entries in the ARP table: 4.
Total number of Dynamic ARP entries: 0.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 3.
Total number of Static ARP entries: 1.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Maximum limit of Learn ARP entry : 512000.
Maximum configured Learn ARP entry limit : 512000.
Learn ARP Entry Threshold is 409600 and Permit Threshold is 486400.
Total number of Learn ARP entries: 0.
Interface            Entry Count
GigabitEthernet4/7            1
GigabitEthernet4/1.1          1
GigabitEthernet4/1            1
EOBC0/0
```

Table 12describes the fields shown in the display.

Table 12   show arp summary Command Field Descriptions

Field	Description
Total Number of entries in the ARP table	Displays the number of entries in the ARP table.
Total number of Dynamic ARP entries	Displays the number of ARP entries in the dynamic state.
Total number of Incomplete ARP entries	Displays the number of ARP entries in the incomplete state.
Total number of Interface ARP entries	Displays the number of ARP entries on ARP enabled interfaces.
Total number of Static ARP entries	Displays the number of active statically configured ARP entries.
Total number of Alias ARP entries	Displays the number of active statically configured alias entries.
Total number of Simple Application ARP entries	Displays the number of ARP entries in the simple application mode.
Total number of Application Alias ARP entries	Displays the number of ARP entries in the application alias mode.
Total number of Application Timer ARP entries	Displays the number of ARP entries in the application timer mode.

Table 12 show arp summary Command Field Descriptions (continued)

Field	Description
Maximum limit of Learn ARP entry	Displays the allowed maximum limit for the learned ARP entries.
Maximum configured Learn ARP entry limit	Displays the figure the maximum learned ARP entry limit is set to.
Learn ARP Entry Threshold	Displays the value representing 80 percent of the set maximum learned ARP entry limit.
Permit Threshold	Displays the value representing 95 percent of the set maximum learned ARP entry limit.
Total number of Learn ARP entries	Displays the total number of learned ARP entries.
Interface	Lists the names of the ARP enabled interfaces.
Entry Count	Displays the number of ARP entries on each ARP enabled interface

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
ip arp entry learn	Specifies the maximum number of learned ARP entries.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

show ip arp [*ip-address*] [*host-name*] [*mac-address*] [*interface type number*]

Syntax Description	*ip-address*	(Optional) ARP entries matching this IP address are displayed.
	host-name	(Optional) Host name.
	mac-address	(Optional) 48-bit MAC address.
	interface type number	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes EXEC

Command History

Release	Modification
9.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples The following is sample output from the **show ip arp** command:

```
Router# show ip arp

Protocol  Address           Age(min)    Hardware Addr   Type      Interface
Internet  172.16.233.229    -           0000.0c59.f892  ARPA      Ethernet0/0
Internet  172.16.233.218    -           0000.0c07.ac00  ARPA      Ethernet0/0
Internet  172.16.233.19     -           0000.0c63.1300  ARPA      Ethernet0/0
Internet  172.16.233.309    -           0000.0c36.6965  ARPA      Ethernet0/0
Internet  172.16.168.11     -           0000.0c63.1300  ARPA      Ethernet0/0
Internet  172.16.168.254    9           0000.0c36.6965  ARPA      Ethernet0/0
```

Table 13 describes the significant fields shown in the display.

Table 13　　*show ip arp Field Descriptions*

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.

Table 13   show ip arp Field Descriptions (continued)

Field	Description
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: • ARPA • SNAP • SAP
Interface	Indicates the interface associated with this network address.

show ip arp inspection

To display the status of DAI for a specific range of VLANs, use the **show ip arp inspection** command in privileged EXEC mode.

> **show ip arp inspection** [**interfaces** [*interface-name*] | **statistics** [**vlan** *vlan-range*]]

Syntax Description		
interfaces *interface-name*	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface.
statistics	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
vlan *vlan-range*	(Optional) Displays the statistics for the selected range of VLANs.

Defaults   This command has no default settings.

Command Modes   Privileged EXEC

Command History

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

Usage Guidelines   If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed.

If you do not specify the interface name, the trust state and rate limit for all applicable interfaces in the system are displayed.

Examples   This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Router# show ip arp inspection statistics vlan 3

Vlan      Forwarded        Dropped      DHCP Drops     ACL Drops
----      ---------        -------      ----------     ----------
   3          31753         102407          102407              0

Vlan   DHCP Permits    ACL Permits    Source MAC Failures
----   ------------    -----------    -------------------
   3          31753              0                      0

Vlan   Dest MAC Failures    IP Validation Failures
----   -----------------    ----------------------
   3                   0                         0
```

Cisco IOS IP Addressing Services Command Reference

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Router# show ip arp inspection statistics

Vlan       Forwarded        Dropped      DHCP Drops     ACL Drops
----       ---------        -------      ----------     ----------
   1               0              0               0              0
   2               0              0               0              0
   3           68322         220356          220356              0
   4               0              0               0              0
 100               0              0               0              0
 101               0              0               0              0
1006               0              0               0              0
1007               0              0               0              0


Vlan     DHCP Permits      ACL Permits   Source MAC Failures
----     ------------      -----------   -------------------
   1               0              0                 0
   2               0              0                 0
   3           68322              0                 0
   4               0              0                 0
 100               0              0                 0
 101               0              0                 0
1006               0              0                 0
1007               0              0                 0


Vlan   Dest MAC Failures   IP Validation Failures
----   -----------------   ----------------------
   1               0                    0
   2               0                    0
   3               0                    0
   4               0                    0
 100               0                    0
 101               0                    0
1006               0                    0
1007               0                    0
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Router# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan     Configuration    Operation   ACL Match          Static ACL
----     -------------    ---------   ---------          ----------
   1     Enabled          Active

Vlan     ACL Logging      DHCP Logging
----     -----------      ------------
   1     Deny             Deny
```

This example shows how to display the trust state of Fast Ethernet interface 6/3:

```
Router# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)    Burst Interval
---------------  -----------     ----------    --------------
Fa6/1            Untrusted            20                 5
```

This example shows how to display the trust state of the interfaces on the switch:

```
Router# show ip arp inspection interfaces

Interface       Trust State    Rate (pps)
---------------  -----------    ----------
Gi1/1           Untrusted              15
Gi1/2           Untrusted              15
Gi3/1           Untrusted              15
Gi3/2           Untrusted              15
Fa3/3           Trusted              None
Fa3/4           Untrusted              15
Fa3/5           Untrusted              15
Fa3/6           Untrusted              15
Fa3/7           Untrusted              15
```

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	Displays the status of DAI for a specific range of VLANs.

show ip arp inspection log

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

show ip arp inspection log

Syntax Description   This command has no arguments or keywords.

Defaults   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 display the current contents of the log buffer before and after the buffers are cleared:

```
Router# show ip arp inspection log

Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.

  Interface       Vlan   Sender MAC        Sender IP        Num of Pkts
  --------------  -----  ----------------  ---------------  -----------
Fa6/3           1      0002.0002.0002    10.1.1.2          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.3          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.4          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.5          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.6          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.7          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.8          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.9          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.10         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3           1      0002.0002.0002    10.1.1.11         1(12:02:52 UTC Fri Apr 25 2003)
   --              --     --                --               5(12:02:52 UTC Fri Apr 25 2003)
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

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

Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
```

Related Commands	Command	Description
	clear ip arp inspection log	Clear the status of the log buffer.
	show ip arp inspection log	Shows the status of the log buffer.

update arp

To secure dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings, use the **update arp** command in DHCP pool configuration mode. To disable this command and change secure ARP entries to dynamic ARP entries, use the **no** form of this command.

update arp

no update arp

Syntax Description   This command has no keywords or arguments.

Defaults   No default behavior or values.

Command Modes   DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines   The **update arp** DHCP pool configuration command is used to secure ARP table entries and their corresponding DHCP leases. However, existing active leases are not secured. These leases will remain insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

This command can be configured only under the following conditions:

- DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.

- Directly connected clients on LAN interfaces and wireless LAN interfaces.

The configuration of this command is not visible to the client. When this command is configured, secured ARP table entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior. If a secure ARP entry created by the DHCP server must be removed, the **clear ip dhcp binding** command can be used. This command will clear the DHCP binding and secured ARP table entry.

Note   This command does not secure ARP table entries for BOOTP clients.

Examples   The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
ip dhcp pool WIRELESS-POOL
 update arp
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP Server database.