CHAPTER 4

Configuring ARP

This chapter describes how the Address Resolution Protocol (ARP) on the ACE can manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets. The ACE creates an ARP cache entry when it receives an ARP packet or you configure an IP address on the ACE (for example, an IP address for a real server, gateway, or an interface VLAN).

You can also configure static ARP entries for IP to Media Access Control (MAC) translations and ARP inspection to prevent ARP spoofing. ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address if the correct MAC address and the associated IP address are in the static ARP table.

This chapter describes how to configure ARP parameters and enable ARP inspection, and contains the following major sections:

Adding a Static ARP Entry

To add a static ARP entry in the ARP table, use the **arp** command in configuration mode or in interface configuration mode. You can create a static ARP entry at the context level. For bridged interfaces, you must configure static ARP entries in interface configuration mode.

Guidelines and Restrictions:

This topic includes the following guidelines and restrictions:

- When you enable ARP inspection, the ACE compares ARP packets with static ARP entries in the ARP table to determine what action to take. For more information, see the "Enabling ARP Inspection" section.
- The **arp** command in configuration mode allows the configuration of the multicast MAC address for a host. The ACE uses this multicast MAC address while sending packets to the host. However, the ACE does not learn the multicast MAC addresses for a host.
- The ACE supports multicast traffic that passes through it but it does not support the creation of multicast traffic.

The syntax of this command is as follows:

arp *ip_address mac_address*

The arguments are as follows:

- *ip_address*—IP address for an ARP table entry. Enter the IP address in dotted-decimal notation (for example, 172.16.56.76).
- *mac_address*—Hardware MAC address for the ARP table entry. Enter the MAC address in dotted-hexadecimal notation (for example, 00.60.97.d5.26.ab).

For example, to allow ARP responses from the router at 10.1.1.1 with the MAC address 00.02.9a.3b.94.d9, enter the following command:

```
host1/Admin(config)# arp 10.1.1.1 00.02.9a.3b.94.d9
```

To remove a static ARP entry, use the **no arp** command. For example, enter:

```
host1/Admin(config)# no arp 10.1.1.1 00.02.9a.3b.94.d9
```

Enabling ARP Inspection

ARP inspection prevents malicious users from impersonating other hosts or routers, known as ARP spoofing. ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router. The gateway router responds with the gateway router MAC address.

However, the attacker sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router. ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address if the correct MAC address and the associated IP address are in the static ARP table.

ARP inspection operates only on ingress bridged interfaces. By default, ARP inspection is disabled on all interfaces, allowing all ARP packets through the ACE. When you enable ARP inspection, the ACE uses the IP address and interface ID (ifID) of an incoming ARP packet as an index into the ARP table. The ACE then compares the MAC address of the ARP packet with the MAC address in the indexed static ARP entry in the ARP table and takes the following actions:

- If the IP address, source ifID, and MAC address match a static ARP entry, the inspection succeeds and the ACE allows the packet to pass.
- If the IP address and interface of the incoming ARP packet match a static ARP entry, but the MAC address of the packet does not match the MAC address that you configured in that static ARP entry, ARP inspection fails, the ACE drops the packet, and it increments the Inspect Failed counter regardless of whether the **flood** or **no-flood** option is configured.
- If the ARP packet does not match any static entries in the ARP table or there are no static entries in the table, then you can set the ACE to either forward the packet out all interfaces (**flood**) or to drop the packet (**no-flood**). In this case, the source IP address to MAC address mapping is new to the ACE. If you enter the **flood** option, the ACE creates a new ARP entry and marks it as LEARNED. If you enter the **no-flood** option, the ACE drops the ARP packet.

To enable ARP inspection, use the **arp inspection enable** command in configuration mode. The syntax of this command is as follows:

arp inspection enable [**flood | no-flood**]

The options are as follows:

- **flood**—Enables ARP forwarding of nonmatching ARP packets. The ACE forwards all ARP packets to all interfaces in the bridge group. This is the default setting. In the absence of a static ARP entry, this option bridges all packets. With this option, the ACE does not increment the Inspect Failed counter of the **show arp statistics** command.
- **no-flood**—Disables ARP forwarding for the interface and drops nonmatching ARP packets. In the absence of a static ARP entry, this option does not bridge any packets. With this option, the ACE does increment the Inspect Failed counter of the **show arp statistics** command.

For example, to enable ARP inspection and to drop all nonmatching ARP packets, enter:

```
host1/Admin(config)# arp inspection enable no-flood
```

To disable ARP inspection, use the **no arp inspection enable** command. For example, enter:

```
host1/Admin(config)# no arp inspection enable
```

Configuring the ARP Retry Attempts

By default, the number of ARP attempts before the ACE flags any learned and configured hosts as down is 3. To configure the number of ARP retry attempts, use the **arp retries** command in configuration mode. You configure this command per context. The syntax of this command is as follows:

arp retries *number*

The *number* argument is the number of ARP retry attempts. Enter a number from 2 to 15. The default is 3.

For example, to configure a retry attempts at 6, enter:

```
host1/Admin(config)# arp retries 6
```

To reset the number of ARP retry attempts to the default of 3, use the **no arp retries** command. For example, enter:

```
host1/Admin(config)# no arp retries
```

Configuring the ARP Retry Interval

By default, the interval when the ACE sends ARP retry attempts to any learned or configured hosts is 10 seconds. To configure this interval, use the **arp rate** command in configuration mode. You configure this command per context. The syntax of this command is as follows:

arp rate *seconds*

The *seconds* argument is the number of seconds between ARP retry attempts to hosts. Enter a number from 1 to 60. The default is 10.

For example, to configure the retry attempt interval of 15 seconds, enter:

```
host1/Admin(config)# arp rate 15
```

To reset the retry attempt interval to the default of 10 seconds, use the **no arp rate** command. For example, enter:

```
host1/Admin(config)# no arp rate
```

Configuring the ARP Request Interval

By default, the refresh interval for existing ARP entries of configured host addresses is 300 seconds. To configure this interval, use the **arp interval** command in configuration mode. You configure this command per context. The syntax of this command is as follows:

arp interval *seconds*

The *seconds* argument is the number of seconds between each ARP request sent to the host. Enter a number from 15 to 31536000. The default is 300.

Note When you change the ARP request internal for learned hosts and configured hosts, the new timeout does not take effect until the existing time is reached. If you want the new timeout to take effect immediately, enter the **clear arp** command to apply the new ARP interval (see the "Clearing ARP Learned Entries from the ARP Table" section).

For example, to configure a request period of 15 seconds, enter:

```
host1/Admin(config)# arp interval 15
```

To reset the ARP request interval to the default of 300 seconds, use the **no arp interval** command. For example, enter:

```
host1/Admin(config)# no arp interval
```

Enabling the Learning of MAC Addresses

By default, for bridged traffic, the ACE learns MAC addresses from all traffic. For routed traffic, the ACE learns MAC addresses only from ARP response packets or from packets that are destined to the ACE (for example, a ping to a VIP or a ping to a VLAN interface). To enable the ACE to learn MAC addresses from traffic after the command has been disabled, use the **arp learned-mode enable** command in configuration mode. You configure this command per context. This command is enabled by default.

The syntax of this command is as follows:

arp learned-mode enable

For example, to enable the ACE to learn MAC addresses from traffic after the command has been disabled, enter:

```
host1/Admin(config)# arp learned-mode enable
```

To instruct the ACE to forward packets without learning the ARP information, use the **no arp learned-mode enable** command. For example, enter:

```
host1/Admin(config)# no arp learned-mode enable
```

Enabling Source MAC Validation

Source MAC validation allows you to instruct the ACE to check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE on the specified interface. The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, source MAC validation is disabled.

Note If ARP inspection fails, then the ACE does not perform source MAC validation. For details about ARP inspection, see the "Enabling ARP Inspection" section.

To configure source MAC validation, use the **arp inspection** command in interface configuration mode. The syntax of this command is:

arp inspection validate src-mac [**flood** | **no-flood**]

The options are as follows:

- **flood**—Enables ARP forwarding for the interface and forwards ARP packets with nonmatching source MAC addresses to all interfaces in the bridge group. This is the default option when you enable source MAC validation.
- **no-flood**—Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.

Note Regardless of whether you enter the **flood** or the **no-flood** option, if the source MAC address of the ARP packet does not match the MAC address of the Ethernet header, then the source MAC validation fails and the ACE increments the Smac-validation Failed counter of the **show arp statistics** command.

For example, to enable source MAC validation and instruct the ACE to drop ARP packets with nonmatching source MAC addresses, enter the following command:

```
host1/Admin(config-if)# arp inspection validate src-mac no-flood
```

To disable source MAC validation, enter the following command:

```
host1/Admin(config-if)# no arp inspection validate src-mac no-flood
```

Configuring the ARP Learned Interval

By default, the refresh interval for existing ARP entries for learned host addresses is 14400 seconds. To configure this interval, use the **arp learned-interval** command in configuration mode. You configure this command per context. The syntax of this command is as follows:

arp learned-interval *seconds*

The *seconds* argument is the number of seconds between ARP requests for learned addresses. Enter a number from 60 to 31536000. The default is 14400.

For example, to configure a learned interval of 800 seconds, enter:

```
host1/Admin(config)# arp learned-interval 800
```

To reset the learned interval to the default of 14,400 seconds, use the **no arp learned-interval** command. For example, enter:

```
host1/Admin(config)# no arp learned-interval
```

Disabling the Replication of ARP Entries

By default, ARP entry replication is enabled. To disable the replication of ARP entries, use the **arp sync disable** command in configuration mode.

The syntax of this command is as follows:

arp sync disable

For example, to disable the replication of ARP entries, enter:

```
host1/Admin(config)# arp sync disable
```

To reenable ARP entry replication, use the **no arp sync disable** command. For example, enter:

```
host1/Admin(config)# no arp sync disable
```

Specifying a Time Interval Between ARP Sync Messages

By default, the time interval between ARP synchronization messages for learned hosts is 5 seconds. To specify this time interval, use the **arp sync-interval** command in configuration mode.

The syntax of this command is as follows:

arp sync-interval *number*

The *number* argument defines the time interval. Enter an integer from 1 to 3600 seconds (1 hour). The default is 5 seconds.

For example, to specify a time interval of 100 seconds, enter:

```
host1/Admin(config)# arp sync-interval 100
```

To restore the default value of 5 seconds, use the **no arp sync-interval** command. For example, enter:

```
host1/Admin(config)# no arp sync-interval
```

Configuring the Rate Limit for Gratuitous ARP Packets

By default, the rate limit for gratuitous ARPs sent by the ACE is 512 packets per second. To configure this rate limit, use the **arp ratelimit** command in configuration mode. This command is available only in the Admin context. This rate limit applies to the module and not per context.

The syntax of this command is as follows:

arp ratelimit *number*

The *number* argument defines the rate limit as packets per second. Enter an integer from 100 to 8192. The default is 512.

Note The rate limit applies to all gratuitous ARPs sent for local addresses on new configurations, module reboot, and on MAC address changes.

For example, to specify a rate limit of 1000 packets per second, enter:

```
host1/Admin(config)# arp ratelimit 1000
```

To restore the default value of 512 packets per second, use the **no arp ratelimit** command. For example, enter:

```
host1/Admin(config)# no arp ratelimit
```

Displaying ARP Information

You can display ARP address mapping, statistics, and timeout intervals. For more information, see the following topics:

- Displaying IP Address-to-MAC Address Mapping
- Displaying ARP Statistics
- Displaying ARP Inspection Configuration
- Displaying ARP Timeout Values

Note The **show arp internal** command is used for debugging purposes. The output for this command is for use by trained Cisco personnel as an aid in debugging and troubleshooting the ACE. For information on the command syntax, see the *Cisco Application Control Engine Module Command Reference*.

Displaying IP Address-to-MAC Address Mapping

To display the current active IP address-to-MAC address mapping in the ARP table, use the **show arp** command in Exec mode. The syntax of this command is as follows:

show arp

Table 4-1 describes the fields in the **show arp** command output.

Table 4-1 Field Descriptions for the show arp Command

Field	Description
Context	Current context.
IP ADDRESS	IP address of the system for ARP mapping.
MAC-ADDRESS	MAC address of the system mapped to the IP address.
Interface	Interface name for this entry.
Type	Type of ARP entry. The possible types are LEARNED, GATEWAY, INTERFACE, VSERVER, RSERVER, and NAT.
Encap	Pointer to the adjacency entry, if any, for this host; Layer 2 and switch header rewrite information.
Next ARP(s)	Time in seconds that this dynamic ARP entry is valid.
Status	State of the system. The possible values are up or down.

For example, enter:

```
host1/admin# show arp
```

Displaying ARP Statistics

To display the ARP statistics globally or for a specified VLAN, use the **show arp statistics** command in Exec mode. The syntax of this command is as follows:

show arp statistics [**vlan** *vlan_number*]

The optional *vlan_number* argument displays the ARP statistics for the specified VLAN. Without this option, this command displays the ARP statistics for all VLAN interfaces.

Table 4-2 describes the fields in the **show arp statistics** command output.

Table 4-2 Field Descriptions for the show arp statistics Command Output

Field	Description
RX Packets	ARP packets received.
RX Errors	Number of errors on received ARP packets.
TX Packets	ARP packets transmitted.
TX Errors	Number of errors on transmitted ARP packets.
Bridged Packets	Number of bridged ARP packets.
Bridged Errors	Number of bridged errors.
Requests Recvd	ARP requests received.
Requests Sent	Number of ARP requests sent.
Response Recvd	ARP responses received.
Response Sent	Number of ARP responses sent.
Packets Dropped	Number of dropped ARP packets.
Inspect Failed	Number of packets failing ARP inspection.
Collision Detected	Number of detected collisions.
Gratuitous ARP sent	Number of gratuitous ARP packets sent.
Hosts learned	Number of hosts learned.
Smac-validation failed	Number of times that the ACE detected a mismatch between the source MAC address in an Ethernet header and the sender's MAC address in an ARP payload of a received ARP packet.
Resolution requests	Number of resolution requests.
Encap-miss msg	Number of packets that contain no matching ARP entry; each learned ARP entry should correspond to an Encap. When a packet does not have a matching entry, the ACE considers it an Encap miss.

Table 4-2 Field Descriptions for the show arp statistics Command Output (continued)

Field	Description
Pings attempted for Encap-miss msg	Number of times that the ACE recognizes that a ping attempt needs to occur when an Encap miss for a destination packet IP address not on an existing bridge-group subnet occurs.
Pings quenched for Encap-miss msg	Number of times that the ACE suppresses an effort to ping for the same destination packet IP address if the Encap miss for that address occurs repeatedly and too fast.
Pings rejected for Encap-miss msg	Number of times that the ACE rejects ping attempts for destination IP addresses when the Encap misses for that address are too many to handle. Similar to the quenched pings, these misses are unique.
Pings Encap-miss responded to	Number of actual pings sent for a missed IP address. The number of this counter should match the number of pings that were attempted for the Encap-miss msg counter.
Replication Counters	
Msg Received	Number of ARP replication messages that were received by the standby ACE.
Hosts Replicated	Number of hosts for which ARP replication succeeded and entries were created on the standby.
Replication Failed	Number of hosts for which replication failed on the standby ACE.
Replication Ignored	Number of hosts for which replication messages were ignored on the standby, possibly because the entries are already present.

For example, enter:

```
host1/admin# show arp statistics
```

You can also display ARP traffic statistics by using the **show ip traffic** command. This command displays the number of received and sent packets, and associated errors, requests, and responses.

Displaying ARP Inspection Configuration

To display the ARP inspection configuration, use the **show arp inspection** command in Exec mode. The syntax of this command is as follows:

show arp inspection

Table 4-3 describes the fields in the **show arp inspection** command output.

Table 4-3 Field Descriptions for the show arp inspection Command

Field	Description
Context	Name of the current context.
ARP Inspection	Status of whether ARP inspection is enabled.
Flooding	Status of whether flooding is enabled.

Displaying ARP Timeout Values

To display the ARP timeout values, use the **show arp timeout** command in Exec mode. The syntax of this command is as follows:

show arp timeout

Table 4-4 describes the fields in the **show arp timeout** command output.

Table 4-4 Field Descriptions for the show arp timeout Command

Field	Description
Refresh Time	Interval in seconds between ARP requests sent to the ACE to validate the cache entry.
Learned Address	Interval in seconds when the ACE sends ARP requests for learned hosts.
Configured Address	Interval in seconds that the ACE sends ARP refresh requests for configured hosts. By default, the interval is 300 seconds.
Retry Rate	Interval in seconds when the ACE sends ARP retry attempts to hosts.
Max Retries per Host	Number of ARP attempts before the ACE flags the host as down.

Clearing ARP Learned Entries from the ARP Table

To clear the ARP learned entries from the ARP cache table, use the **clear arp** command. The syntax of this command is as follows:

clear arp [**no-refresh**]

The optional **no-refresh** keyword clears the learned ARP entries in the cache table without performing an ARP on the entries. Without this option, this command performs an ARP on the entries.

For example, to clear the ARP learned entries with a re-ARP on the entries, enter:

```
host1/Admin# clear arp
```

Clearing ARP Statistics

To clear the ARP statistics counters, use the **clear arp statistics** command. The syntax of this command is as follows:

clear arp statistics [**vlan** *number*]

The optional **vlan** *number* argument clears the statistic counters for the specified interface. Without this option, this command clears all counters for all interfaces.

For example, to clear the ARP statistics counters globally, enter:

```
host1/Admin# clear arp statistics
```