



CHAPTER 24

Configuring ARP Inspection and Bridging Parameters in Transparent Mode

This chapter describes how to enable ARP inspection and how to customize bridging operations for the adaptive security appliance in transparent firewall mode. In multiple context mode, the commands in this chapter can be entered in a security context, but not the system.

This chapter includes the following sections:

- [Configuring ARP Inspection, page 24-1](#)
- [Customizing the MAC Address Table, page 24-3](#)

Configuring ARP Inspection

This section describes ARP inspection and how to enable it, and includes the following topics:

- [ARP Inspection Overview, page 24-1](#)
- [Adding a Static ARP Entry, page 24-2](#)
- [Enabling ARP Inspection, page 24-2](#)

ARP Inspection Overview

By default, all ARP packets are allowed through the adaptive security appliance. You can control the flow of ARP packets by enabling ARP inspection.

When you enable ARP inspection, the adaptive security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the adaptive security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the adaptive security appliance to either forward the packet out all interfaces (flood), or to drop the packet.

**Note**

The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

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. The attacker, however, 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, so long as the correct MAC address and the associated IP address are in the static ARP table.

Adding a Static ARP Entry

ARP inspection compares ARP packets with static ARP entries in the ARP table. Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver. The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

**Note**

The transparent firewall uses dynamic ARP entries in the ARP table for traffic to and from the adaptive security appliance, such as management traffic.

To add a static ARP entry, enter the following command:

```
hostname(config)# arp interface_name ip_address mac_address
```

For example, to allow ARP responses from the router at 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface, enter the following command:

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Enabling ARP Inspection

To enable ARP inspection, enter the following command:

```
hostname(config)# arp-inspection interface_name enable [flood | no-flood]
```

Where **flood** forwards non-matching ARP packets out all interfaces, and **no-flood** drops non-matching packets.

**Note**

The default setting is to flood non-matching packets. To restrict ARP through the adaptive security appliance to only static entries, then set this command to **no-flood**.

For example, to enable ARP inspection on the outside interface, and to drop all non-matching ARP packets, enter the following command:

```
hostname(config)# arp-inspection outside enable no-flood
```

To view the current settings for ARP inspection on all interfaces, enter the **show arp-inspection** command.

Customizing the MAC Address Table

This section describes the MAC address table, and includes the following topics:

- [MAC Address Table Overview, page 24-3](#)
- [Adding a Static MAC Address, page 24-4](#)
- [Setting the MAC Address Timeout, page 24-4](#)
- [Disabling MAC Address Learning, page 24-4](#)
- [Viewing the MAC Address Table, page 24-4](#)

MAC Address Table Overview

The adaptive security appliance learns and builds a MAC address table in a similar way as a normal bridge or switch: when a device sends a packet through the adaptive security appliance, the adaptive security appliance adds the MAC address to its table. The table associates the MAC address with the source interface so that the adaptive security appliance knows to send any packets addressed to the device out the correct interface.

Because the adaptive security appliance is a firewall, if the destination MAC address of a packet is not in the table, the adaptive security appliance does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly connected devices or for remote devices:

- Packets for directly connected devices—The adaptive security appliance generates an ARP request for the destination IP address, so that the adaptive security appliance can learn which interface receives the ARP response.
- Packets for remote devices—The adaptive security appliance generates a ping to the destination IP address so that the adaptive security appliance can learn which interface receives the ping reply.

The original packet is dropped.



Note

In transparent firewall mode, the management interface updates the MAC address table in the same manner as a data interface; therefore you should not connect both a management and a data interface to the same switch unless you configure one of the switch ports as a routed port (by default Cisco Catalyst switches share a MAC address for all VLAN switch ports). Otherwise, if traffic arrives on the management interface from the physically-connected switch, then the adaptive security appliance updates the MAC address table to use the *management* interface to access the switch, instead of the data interface. This action causes a temporary traffic interruption; the adaptive security appliance will not re-update the MAC address table for packets from the switch to the data interface for at least 30 seconds for security reasons.

Adding a Static MAC Address

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the adaptive security appliance drops the traffic and generates a system message. When you add a static ARP entry (see the “[Adding a Static ARP Entry](#)” section on page 24-2), a static MAC address entry is automatically added to the MAC address table.

To add a static MAC address to the MAC address table, enter the following command:

```
hostname(config)# mac-address-table static interface_name mac_address
```

The *interface_name* is the source interface.

Setting the MAC Address Timeout

The default timeout value for dynamic MAC address table entries is 5 minutes, but you can change the timeout. To change the timeout, enter the following command:

```
hostname(config)# mac-address-table aging-time timeout_value
```

The *timeout_value* (in minutes) is between 5 and 720 (12 hours). 5 minutes is the default.

Disabling MAC Address Learning

By default, each interface automatically learns the MAC addresses of entering traffic, and the adaptive security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired, however, unless you statically add MAC addresses to the table, no traffic can pass through the adaptive security appliance.

To disable MAC address learning, enter the following command:

```
hostname(config)# mac-learn interface_name disable
```

The **no** form of this command reenables MAC address learning. The **clear configure mac-learn** command reenables MAC address learning on all interfaces.

Viewing the MAC Address Table

You can view the entire MAC address table (including static and dynamic entries for both interfaces), or you can view the MAC address table for an interface. To view the MAC address table, enter the following command:

```
hostname# show mac-address-table [interface_name]
```

The following is sample output from the **show mac-address-table** command that shows the entire table:

```
hostname# show mac-address-table
interface          mac address          type      Time Left
-----
outside           0009.7cbe.2100      static    -
inside            0010.7cbe.6101      static    -
inside            0009.7cbe.5101      dynamic   10
```

The following is sample output from the **show mac-address-table** command that shows the table for the inside interface:

```
hostname# show mac-address-table inside
interface      mac address      type      Time Left
-----
inside         0010.7cbe.6101   static    -
inside         0009.7cbe.5101   dynamic   10
```

