



## CHAPTER 30

# Configuring ARP Inspection and Bridging Parameters

---

This chapter describes how to enable ARP inspection and how to customize bridging operations for the 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.

For information about transparent firewall mode, see [Chapter 18, “Firewall Mode Overview.”](#)

This chapter includes the following sections:

- [Configuring ARP Inspection, page 30-1](#)
- [Customizing the MAC Address Table, page 30-4](#)

## Configuring ARP Inspection

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

- [ARP Inspection, page 30-1](#)
- [Edit ARP Inspection Entry, page 30-2](#)
- [ARP Static Table, page 30-3](#)
- [Add/Edit ARP Static Configuration, page 30-4](#)

## ARP Inspection

The ARP Inspection pane lets you configure ARP inspection.

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

When you enable ARP inspection, the 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 security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the 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.

#### Fields

- Interface—Shows the interface names.
- ARP Inspection Enabled—Shows if ARP inspection is enabled, Yes or No.
- Flood Enabled—If ARP inspection is enabled, shows if the action is to flood unknown packets, Yes or No. If ARP inspection is disabled, this value is always No.
- Edit—Edits the ARP inspection parameters for the selected interface.

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

## Edit ARP Inspection Entry

The Edit ARP Inspection Entry dialog box lets you set ARP inspection settings.

#### Fields

- Enable ARP Inspection—Enables ARP inspection.
- Flood ARP Packets—Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet. If you do not check this check box, all non-matching packets are dropped.



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

The Management 0/0 interface or subinterface, if present, never floods packets even if this parameter is set to flood.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

## ARP Static 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 security appliance, such as management traffic.

The ARP Static Table panel lets you add static ARP entries that map a MAC address to an IP address for a given interface. Static ARP entries do not time out, and might help you solve a networking problem.

**Fields**

- Interface—Shows the interface attached to the host network.
- IP Address—Shows the host IP address.
- MAC Address—Shows the host MAC address.
- Proxy ARP—Shows whether the security appliance performs proxy ARP for this address. If the security appliance receives an ARP request for the specified IP address, then it responds with the specified MAC address.
- Add—Adds a static ARP entry.
- Edit—Edits a static ARP entry.
- Delete—Deletes a static ARP entry.
- ARP Timeout—Sets the amount of time before the security appliance rebuilds the ARP table, between 60 to 4294967 seconds. The default is 14400 seconds. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently. Although this parameter appears on the ARP Static Table panel, the timeout applies to the *dynamic* ARP table.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit ARP Static Configuration

The Add/Edit ARP Static Configuration dialog box lets you add or edit a static ARP entry.

### Fields

- Interface—Sets the interface attached to the host network.
- IP Address—Sets the host IP address.
- MAC Address—Sets the host MAC address; for example, 00e0.1e4e.3d8b.
- Proxy ARP—Enables the security appliance to perform proxy ARP for this address. If the security appliance receives an ARP request for the specified IP address, then it responds with the specified MAC address.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Customizing the MAC Address Table

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

- [MAC Address Table, page 30-4](#)
- [Add/Edit MAC Address Entry, page 30-6](#)
- [MAC Learning, page 30-6](#)

## MAC Address Table

The MAC Address Table pane lets you add static MAC Address entries. 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 security appliance

drops the traffic and generates a system message. When you add a static ARP entry (see the “[ARP Static Table](#)” section on page 30-3), a static MAC address entry is automatically added to the MAC address table.

The 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 security appliance, the security appliance adds the MAC address to its table. The table associates the MAC address with the source interface so that the security appliance knows to send any packets addressed to the device out the correct interface.

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 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 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.

The ASA 5505 adaptive security appliance includes a built-in switch; the switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN. This section discusses the bridge MAC address table, which maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

Because the security appliance is a firewall, if the destination MAC address of a packet is not in the table, the 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 security appliance generates an ARP request for the destination IP address, so that the security appliance can learn which interface receives the ARP response.
- Packets for remote devices—The security appliance generates a ping to the destination IP address so that the security appliance can learn which interface receives the ping reply.

The original packet is dropped.

### Fields

- Interface—Shows the interface associated with the MAC address.
- MAC Address—Shows the MAC address.
- Add—Adds a static MAC address entry.
- Edit—Edits a static MAC address entry.
- Delete—Deletes a static MAC address entry.
- Dynamic Entry Timeout—Sets the time a MAC address entry stays in the MAC address table before timing out, between 5 and 720 minutes (12 hours). 5 minutes is the default.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

## Add/Edit MAC Address Entry

The Add/Edit MAC Address Entry dialog box lets you add or edit a static MAC address entry. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. 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 security appliance drops the traffic and generates a system message.

### Fields

- Interface Name—Sets the interface associated with the MAC address.
- MAC Address—Sets the MAC address.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

## MAC Learning

The MAC Learning pane lets you disable MAC address learning on an interface. By default, each interface automatically learns the MAC addresses of entering traffic, and the 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 security appliance.

### Fields

- Interface—Shows the interface name.
- MAC Learning Enabled—Shows if MAC learning is enabled, Yes or No.
- Enable—Enables MAC learning to the selected interface.
- Disable—Disables MAC learning to the selected interface.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
—	•	•	•	—

