



Configuring Bridging Parameters and ARP Inspection

Transparent firewall mode only

This chapter tells how to customize bridging operations and how to enable ARP inspection for the transparent firewall. This chapter includes the following sections:

- [Customizing the MAC Address Table, page 7-1](#)
- [Configuring ARP Inspection, page 7-3](#)

Customizing the MAC Address Table

This section includes the following topics:

- [MAC Address Table Overview, page 7-1](#)
- [Adding a Static MAC Address, page 7-2](#)
- [Setting the MAC Address Timeout, page 7-2](#)
- [Disabling MAC Address Learning, page 7-2](#)
- [Viewing the MAC Address Table, page 7-3](#)

MAC Address Table Overview

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

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

The original packet is dropped.

**Note**

For multiple context mode, you can limit the maximum number of mac address table entries in the context class. See the “[Configuring a Class](#)” section on page 5-14 for more information.

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.

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

```
FWSM/contexta(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:

```
FWSM/contexta(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 FWSM adds corresponding entries to the MAC address table. You can disable MAC address learning if desired.

To disable MAC address learning, enter the following command:

```
FWSM/contexta(config)# mac-learn interface_name disable
```

The **no** form of this command reenables MAC address learning.

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:

```
FWSM/contexta# show mac-address-table [interface_name]
```

The following example shows the entire MAC address table:

```
FWSM/contexta# 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 example shows the MAC address table for the inside interface:

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

Configuring ARP Inspection

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

- [ARP Inspection Overview, page 7-3](#)
- [Adding a Static ARP Entry, page 7-4](#)
- [Enabling ARP Inspection, page 7-4](#)

ARP Inspection Overview

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the FWSM.

When you enable ARP inspection, the FWSM 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 FWSM drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the FWSM to either forward the packet out all interfaces (flood), or to drop the packet.

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.

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

```
FWSM/contexta(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:

```
FWSM/contexta(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Enabling ARP Inspection

To enable ARP inspection, enter the following command:

```
FWSM/contexta(config)# arp-inspection interface_name enable [flood | no-flood]
```

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

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

```
FWSM/contexta(config)# arp-inspection outside enable no-flood
```