Understanding and Configuring Dynamic ARP Inspection

This chapter describes how to configure Dynamic ARP Inspection (DAI) on the Catalyst 4500 series switch.

This chapter includes the following major sections:

Note For complete syntax and usage information for the switch commands used in this chapter, first look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

If the command is not found in the *Catalyst 4500 Command Reference*, it will be found in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

Overview of Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain "man-in-the-middle" attacks.

This section contains the following subsections:

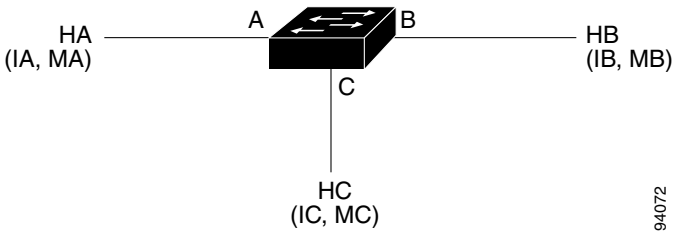
- Port Channels and Their Behavior, page 29-5

ARP Cache Poisoning

You can attack hosts, switches, and routers connected to your Layer 2 network by "poisoning" their ARP caches. For example, a malicious user might intercept traffic intended for other hosts on the subnet by poisoning the ARP caches of systems connected to the subnet.

Consider the following configuration:

Figure 29-1 ARP Cache Poisoning



Hosts HA, HB, and HC are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host HA uses IP address IA and MAC address MA. When HA needs to communicate to HB at the IP Layer, HA broadcasts an ARP request for the MAC address associated with IB. As soon as HB receives the ARP request, the ARP cache on HB is populated with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When HB responds, the ARP cache on HA is populated with a binding for a host with the IP address IB and a MAC address MB.

Host HC can "poison" the ARP caches of HA and HB by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that HC intercepts that traffic. Because HC knows the true MAC addresses associated with IA and IB, HC can forward the intercepted traffic to those hosts using the correct MAC address as the destination. HC has inserted itself into the traffic stream from HA to HB, the classic "man in the middle" attack.

Dynamic ARP Inspection

To prevent ARP poisoning attacks such as the one described in the previous section, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

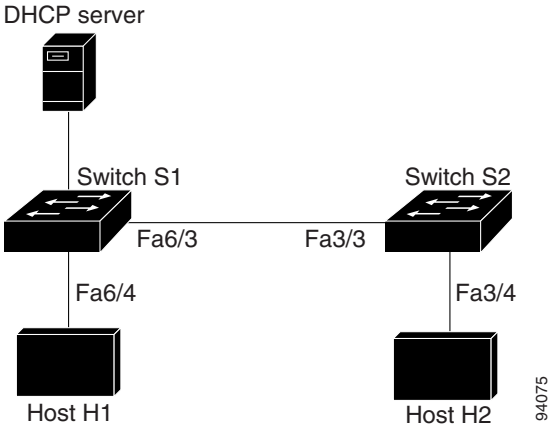
DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided that it is enabled on the VLANs and on the switch in question. In addition, DAI can also validate ARP packets against user-configured ARP ACLs in order to handle hosts that use statically configured IP addresses.

DAI can also be configured to drop ARP packets when the IP addresses in the packet are invalid or when the MAC addresses in the body of the ARP packet do not match the addresses specified in the Ethernet header.

Interface Trust state, Security Coverage and Network Configuration

DAI associates a trust state with each interface on the system. Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process. In a typical network configuration for DAI, all ports connected to host ports are configured as untrusted, while all ports connected to switches are configured as trusted. With this configuration, all ARP packets entering the network from a given switch will have passed the security check; it is unnecessary to perform a validation at any other place in the VLAN / network:

Figure 29-2 Validation of ARP Packets on a DAI-enabled VLAN



Use the trust state configuration carefully.

Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity. If we assume that both S1 and S2 (in Figure 29-2) run DAI on the VLAN that holds H1 and H2, and if H1 and H2 were to acquire their IP addresses from S1, then only S2 binds the IP to MAC address of H1. Therefore, if the interface between S1 and S2 is untrusted, the ARP packets from H1 get dropped on S2. This condition would result in a loss of connectivity between H1 and H2.

Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If S1 were not running DAI, then H1 can easily poison the ARP of S2 (and H2, if the inter-switch link is configured as trusted). This condition can occur even though S2 is running DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a switch running DAI do not poison the ARP caches of other hosts in the network. It does not, however, ensure that hosts from other portions of the network do not poison the caches of the hosts connected to it.

To handle cases in which some switches in a VLAN run DAI and other switches do not, the interfaces connecting such switches should be configured as untrusted. To validate the bindings of packets from non-DAI switches, however, the switch running DAI should be configured with ARP ACLs. When it is not feasible to determine such bindings, switches running DAI should be isolated from non-DAI switches at Layer 3.

Note Depending on the setup of DHCP server and the network, it may not be possible to perform validation of a given ARP packet on all switches in the VLAN.

Relative Priority of Static Bindings and DHCP Snooping Entries

As mentioned previously, DAI populates its database of valid MAC address to IP address bindings through DHCP snooping. It also validates ARP packets against statically configured ARP ACLs. It is important to note that ARP ACLs have precedence over entries in the DHCP snooping database. ARP Packets are first compared to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, then the packet will be denied even if a valid binding exists in the database populated by DHCP snooping.

Logging of Denied Packets

DAI maintains a log of denied IP ARP packets. Log messages are generated at a controlled rate, and log entries are cleared once messages are generated on their behalf.

Rate Limiting of ARP Packets

DAI performs validation checks in the CPU, so the number of incoming ARP packets is rate-limited to prevent a denial of service attack. By default, the rate for untrusted interfaces is set to 15 packets per second, whereas trusted interfaces have no rate limit. When the rate of incoming ARP packets exceeds the configured limit, the port is placed in the errdisable state. The port remains in that state until an administrator intervenes. You can enable errdisable recovery so that ports emerge from this state automatically after a specified timeout period.

Unless a rate limit is explicitly configured on an interface, changing the trust state of the interface will also change its rate limit to the default value for that trust state; that is, 15 packets per second for untrusted interfaces and unlimited for trusted interfaces. Once a rate limit is configured explicitly, the interface retains the rate limit even when its trust state is changed. At any time, the interface reverts to its default rate limit if the no form of the **rate limit** command is applied.

Port Channels and Their Behavior

A given physical port can join a channel only when the trust state of the physical port and of the channel match. Otherwise, the physical port remains suspended in the channel. A channel inherits its trust state from the first physical port that joined the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

Conversely, when the trust state is changed on the channel, the new trust state is configured on all the physical ports that comprise the channel.

The rate limit check on port channels is unique. The rate of incoming packets on a physical port is checked against the port channel configuration rather than the physical ports configuration.

The rate limit configuration on a port channel is independent of the configuration on its physical ports.

The rate limit is cumulative across all physical port; that is, the rate of incoming packets on a port channel equals the sum of rates across all physical ports.

When you configure rate limits for ARP packets on trunks, you must account for VLAN aggregation because a high rate limit on one VLAN can cause a “denial of service” attack to other VLANs when the port is errdisabled by software. Similarly, when a port channel is errdisabled, a high rate limit on one physical port can cause other ports in the channel to go down.

Configuring Dynamic ARP Inspection

This section includes these scenarios:

Scenario One: Two Switches Support Dynamic ARP Inspection

Assume that there are two switches, S1 and S2 with hosts H1 and H2 attached, respectively. Both S1 and S2 are running DAI on VLAN 1 where the hosts are located. The S1 interface fa6/3 is connected to the S2 interface fa3/3, and a DHCP server is connected to S1. Both hosts acquire their IP addresses from the same DHCP server. Therefore, S1 has the binding for H1 and H2, and S2 has the binding for host H2.

To make the setup effective, you must configure the interface fa3/3 on S2 to be trusted. (You can leave interface fa6/3 on S1 as untrusted.) If the DHCP server is moved from S1 to a different location, however, the configuration will not work. To ensure that this setup works permanently, without compromising security, you must configure both interfaces fa6/3 on S1 and fa3/3 on S2 as trusted.

Configuring Switch S1

To enable DAI and configure fa6/3 on S1 as trusted, follow these steps:

Step 1 Verify the connection between switches S1 and S2:

```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 6/3            177         R S I     WS-C4006  Fas 3/3
S1#
```

Step 2 Enable DAI on VLAN 1 and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# ip arp inspection vlan 1
S1(config)# end
S1# 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
S1#
```

Step 3 Configure interface fa6/3 as trusted:

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# in fa6/3
S1(config-if)# ip arp inspection trust
S1(config-if)# end
S1# show ip arp inspection interfaces fastEthernet 6/3

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted              None
S1#
```

Step 4 Verify the bindings:

```
S1# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:00:02:00:02   1.1.1.2          4993        dhcp-snooping  1     FastEthernet6/4
S1#
```

Step 5 Check the statistics before and after Dynamic ARP processes any packets:

```
S1# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
S1#
```

If H1 then sends out two ARP requests with an IP address of 1.1.1.2 and a MAC address of 0002.0002.0002, both requests are permitted, as reflected in the following statistics:

```
S1# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
S1#
```

If H1 then tries to send an ARP request with an IP address of 1.1.1.3, the packet is dropped and an error message is logged:

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa6/4, vlan
1.([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])
S1# show ip arp inspection statistics vlan 1
S1#
```

The statistics will display as follows:

```
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              2              2             0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
S1#
```

Configuring Switch S2

To enable DAI and configure fa3/3 on S2 as trusted, follow these steps:

Step 1 Verify the connectivity:

```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 3/3            120         R S I     WS-C4006  Fas 6/3
S2#
```

Step 2 Enable DAI on VLAN 1, and verify the configuration:

```
S2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# ip arp inspection vlan 1
S2(config)# end
S2# 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
S2#
```

Step 3 Configure interface fa3/3 as trusted:

```
S2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface fastEthernet 3/3
S2(config-if)# ip arp inspection trust
S2(config-if)# end
S2# 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

<output truncated>
S2#
```

Step 4 Verify the list of DHCP snooping bindings:

```
S2# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          4995        dhcp-snooping  1     FastEthernet3/4
S2#
```

Step 5 Check the statistics before and after Dynamic ARP processes any packets:

```
S2# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
S2#
```

If H2 then sends out an ARP request with the IP address 1.1.1.1 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated appropriately:

```
S2# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              1              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
S2#
```

Conversely, if H2 attempts to send an ARP request with the IP address 1.1.1.2, the request is dropped and an error message is logged:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/4, vlan
1.([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri May 23 2003])
S2#
```

The statistics will display as follows:

```
S2# show ip arp inspection statistics vlan 1

Vlan      Forwarded         Dropped     DHCP Drops     ACL Drops
 ----      ---------         -------     ----------     ----------
    1              1               1              1              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
S2#
```

Scenario Two: One Switch Supports Dynamic ARP Inspection

If switch S2 does not support DAI or DHCP snooping, configuring interface fa6/3 as trusted would leave a security hole because both S1 and H1 could be attacked by either S2 or H2. To prevent this possibility, you must configure interface fa6/3 as untrusted. To permit ARP packets from H2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of H2 is not static, such that it is impossible to apply the ACL configuration on S1, S1 and S2 must be separated at Layer 3, that is, have a router routing packets between S1 and S2.

To set up an ARP ACL on switch S1, follow these steps:

Step 1 Set up the access list to permit the IP address 1.1.1.1 and the MAC address 0001.0001.0001, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# arp access-list H2
S1(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
S1(config-arp-nacl)# end
S1# show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 0001.0001.0001
```

Step 2 Apply the ACL to VLAN 1, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# ip arp inspection filter H2 vlan 1
S1(config)# end
S1#

S1# 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      H2                 No
```

```
 Vlan     ACL Logging       DHCP Logging
 ----     -----------       ------------
    1     Deny              Deny
S1#
```

Step 3 Establish the interface fa6/3 as untrusted, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# in fa6/3
S1(config-if)# no ip arp inspection trust
S1(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3

 Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Untrusted               15

Switch#
```

When H2 sends 5 ARP requests through interface fa6/3 on S1 and a “get” is permitted by S1, the statistics are updated appropriately:

```
Switch# show ip arp inspection statistics vlan 1
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              5              0              0              0
Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              5                    0
Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
Switch#
```