CHAPTER 22

Configuring Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol inspection (dynamic ARP inspection) on the switch. This feature helps prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

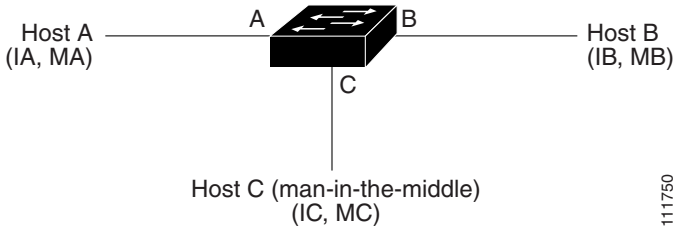
This chapter consists of these sections:

Understanding Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 22-1 shows an example of ARP cache poisoning.

Figure 22-1 ARP Cache Poisoning



subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches 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 Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B 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 Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic *man-in-the middle*

received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-VLAN basis by using the **ip arp inspection vlan** *vlan-range* “Configuring Dynamic ARP Inspection in DHCP Environments” section on page 22-7.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the **arp access-list** *acl-name*

” section on page 22-8. The switch logs dropped packets. For more information about the log buffer, see the “Logging of Dropped Packets” section on page 22-4.

You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the **ip arp inspection validate** {[**src-mac**] [ ] [ ]} global configuration command. For more information, see the “Performing Validation Checks” section on page 22-12.

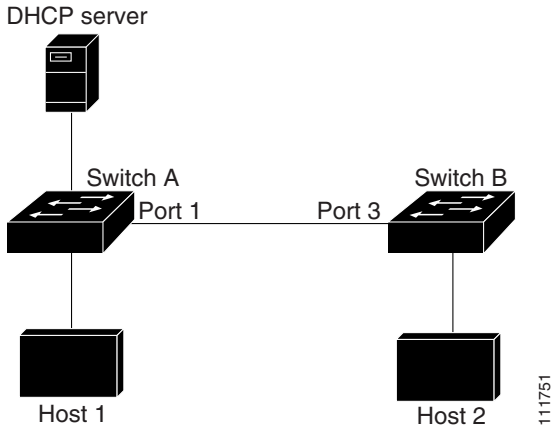
Interface Trust States and Network Security

trust

Caution

, assume that both Switch A and Switch B are running dynamic ARP inspection on the VLAN that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.

ARP Packet Validation on a VLAN Enabled for Dynamic ARP Inspection



inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches

Rate Limiting of ARP Packets

errdisable recovery

page 22-10.

Relative Priority of ARP ACLs and DHCP Snooping Entries

ip arp inspection filter vlan

Logging of Dropped Packets

ip arp inspection log-buffer

ip arp inspection vlan logging

Configuring Dynamic ARP Inspection

-
- Dynamic ARP Inspection Configuration Guidelines, page 22-6

  Configuring Dynamic ARP Inspection in DHCP Environments, page 22-7 (required in DHCP environments)

  Configuring ARP ACLs for Non-DHCP Environments, page 22-8 (required in non-DHCP environments)

  Limiting the Rate of Incoming ARP Packets, page 22-10 (optional)

  Performing Validation Checks, page 22-12 (optional)

  Configuring the Log Buffer, page 22-13 (optional)

Table 22-1 shows the default dynamic ARP inspection configuration.

Table 22-1 Default Dynamic ARP Inspection Configuration

Feature	Default Setting

Dynamic ARP Inspection Configuration Guidelines

-
-
-
-

Note

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

  Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

  The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

  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.

  If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.

  Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

  When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.

Beginning in privileged EXEC mode, follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

	Command	Purpose
Step 1	**show cdp neighbors**	
Step 2		
Step 3	***vlan***	VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.
Step 4	*interface-id*	
Step 5		
Step 6		

	Command	Purpose
Step 7		
Step 8		
Step 9		
Step 10		

```
Switch(config)# ip arp inspection vlan 1
                interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

Configuring ARP ACLs for Non-DHCP Environments

	Command	Purpose
Step 1		
Step 2		Note

Step 3	*sender-ip* *sender-mac*	*sender-ip* *sender-mac*
	exit	
	ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* **static**	*arp-acl-name* *vlan-range* **static**
	interface *interface-id*	

	Command	Purpose
Step 7		
Step 8		
Step 9		
Step 10		

host2

```
                arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
                        exit
                ip arp inspection filter host2 vlan 1
                interface gigabitethernet0/1
                   no ip arp inspection trust
```

Limiting the Rate of Incoming ARP Packets

Note

	Command	Purpose
Step 1		
Step 2		
Step 3	] | }	Limit the rate of incoming ARP requests and responses on the interface. The default rate is 15 pps on untrusted interfaces and unlimited on trusted interfaces. The burst interval is 1 second. The keywords have these meanings: For , specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps. (Optional) For , specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets.The range is 1 to 15. For , specify no upper limit for the rate of incoming ARP packets that can be processed.
		Return to global configuration mode.
		(Optional) Enable error recovery from the dynamic ARP inspection error-disable state. By default, recovery is disabled, and the recovery interval is 300 seconds. For , specify the time in seconds to recover from the error-disable state. The range is 30 to 86400.
		Return to privileged EXEC mode.
		Verify your settings.
		(Optional) Save your entries in the configuration file.

Performing Validation Checks

	Command	Purpose
Step 1		
Step 2		• • •
Step 3		
Step 4		
Step 5		

Configuring the Log Buffer

	Command	Purpose
Step 1		
Step 2	*number* *number* *seconds*	*number* *number* *seconds* *number* *seconds* *number* *seconds* Y, X divided by Y (X/Y) system messages are sent every second. Otherwise, one system message is sent every Y divided by X (Y/X) seconds.

	Command	Purpose
Step 3		• • • • • •
Step 4		
Step 5		
Step 6		

To return to the default log buffer settings, use the { | } global configuration command. To return to the default VLAN log settings, use the { | } global configuration command. To clear the log buffer, use the privileged EXEC command.

Displaying Dynamic ARP Inspection Information

Command	Description

Table 22-3 Commands for Clearing or Displaying Dynamic ARP Inspection Statistics

Table 22-4 Commands for Clearing or Displaying Dynamic ARP Inspection Logging Information
