Dynamic ARP Inspection

Feature history for Dynamic ARP Inspection

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	Dynamic ARP Inspection: Dynamic ARP Inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.	Cisco C9350 Series Smart Switches

Understand Dynamic ARP Inspection

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

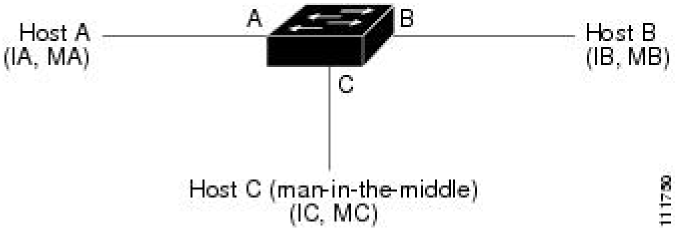
ARP packets in a network

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. This figure shows an example of ARP cache poisoning.

Figure 1: ARP cache poisoning



Hosts A, B, and C 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 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*attack.

How Dynamic ARP Inspection works

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drops invalid ARP packets.

Dynamic ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is 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.

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* global configuration command.

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**] [**dst-mac**] [**ip**]} global configuration command.

Interface trust states and network security

Dynamic ARP inspection associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all Dynamic ARP Inspection validation checks, and those arriving on untrusted interfaces undergo the Dynamic ARP Inspection validation process.

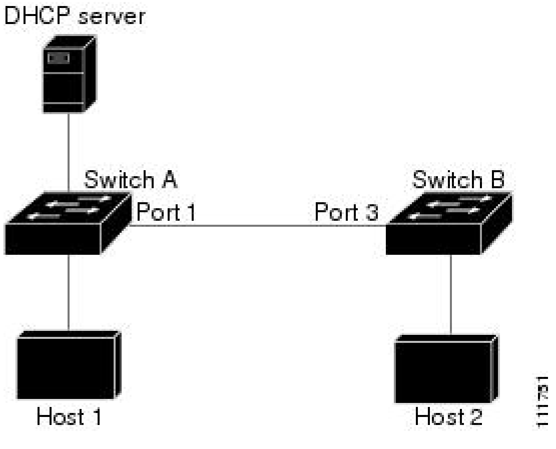
In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed elsewhere in the VLAN or network. You configure the trust setting by using the **ip arp inspection trust interface** configuration command.

⚠

Caution Carefully configure the trust state. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

In the next figure, assume both Switch A and Switch B are running Dynamic ARP Inspection on the VLAN that includes Host 1 and Host 2. When 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.

Figure 2: ARP packet validation on a VLAN enabled for Dynamic ARP Inspection



Trusting interfaces that should be untrusted creates network security gaps. If Switch A is not running Dynamic ARP Inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running Dynamic ARP Inspection.

Dynamic ARP inspection ensures that hosts connected to untrusted interfaces on a switch running Dynamic ARP Inspection do not poison the ARP caches of other hosts in the network. However, Dynamic ARP Inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running Dynamic ARP Inspection.

In cases in which some switches in a VLAN run Dynamic ARP Inspection and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from non-Dynamic ARP Inspection switches, configure the switch running Dynamic ARP Inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches running Dynamic ARP Inspection from switches not running Dynamic ARP Inspection switches.

Note It might not be possible to validate a given ARP packet on all switches in the VLAN, depending on the DHCP server and network setup.

Rate limit of ARP packets

The switch CPU performs Dynamic ARP Inspection validation checks, which limit the number of incoming ARP packets to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. Use the **ip arp inspection limit** interface configuration command to change this setting.

The switch places the port in the error-disabled state when the rate of incoming ARP packets exceeds the configured limit. The port remains in that state until you take action. You can use the **errdisable recovery** global configuration command to enable error disable recovery, allowing ports to automatically emerge from this state after a specified timeout period.

Note For an EtherChannel, the rate limit is applied separately to each switch in a stack. For example, if a limit of 20 pps is configured on the EtherChannel, each switch with ports in the EtherChannel can carry up to 20 pps. If any switch exceeds the limit, the entire EtherChannel is placed into the error-disabled state.

Relative priority of ARP ACLs and DHCP snooping entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take priority over DHCP snooping entries. The switch uses ACLs only if you configure them by using the **ip arp inspection filter vlan** global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch will deny the packet even if a valid binding exists in the database populated by DHCP snooping.

Log dropped packets

When the switch drops a packet, it generates system messages on a rate-controlled basis after placing an entry in the log buffer. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as receiving VLAN, port number, source IP address, destination IP address, source MAC address, and destination MAC address.

Use the **ip arp inspection log-buffer** global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. Use the **ip arp inspection vlan logging** global configuration command to specify the type of packets that are logged.

Default Dynamic ARP Inspection configuration

Feature	Default Settings
Dynamic ARP Inspection	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
Rate limit of incoming ARP packets	The rate is set at 15 pps on untrusted interfaces, assuming network switching with hosts connecting to up to 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.
ARP ACLs for non-DHCP environments	No ARP ACLs are defined.
Validation checks	No checks are performed.
Log buffer	When Dynamic ARP Inspection is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.
Per-VLAN logging	All denied or dropped ARP packets are logged.

Restrictions for Dynamic ARP Inspection

This section lists the restrictions and guidelines for configuring Dynamic Address Resolution Protocol (ARP) Inspection on the switch.

- Dynamic ARP Inspection is an ingress security feature. It does not perform any egress checking.
- Dynamic ARP Inspection is not effective for hosts connected to switches that do not support Dynamic ARP Inspection or that do not have this feature enabled. Man-in-the-middle attacks are limited to a single Layer 2 broadcast domain.

  For security, separate the domain with Dynamic ARP Inspection checks from ones without checking. This action secures the ARP caches of hosts in the domain enabled for Dynamic ARP Inspection.
- Dynamic ARP Inspection verifies IP-to-MAC address bindings by relying on entries in the DHCP snooping binding database for incoming ARP requests and ARP responses.

  Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. Use ARP ACLs to permit or deny packets when DHCP snooping is disabled or in non-DHCP environments.

- Dynamic ARP Inspection supports access ports, trunk ports, and EtherChannel ports only.

Note Do not enable Dynamic ARP Inspection on RSPAN VLANs. Configuring Dynamic ARP Inspection on RSPAN VLANs can obstruct packet delivery to the RSPAN destination port.

- A physical port can join an EtherChannel port channel only if 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 rate limit is calculated separately on each switch in a switch stack. For a cross-stack EtherChannel, this means that the actual rate limit might be higher than the configured value.

  For example, if you set the rate limit to 30 pps on an EtherChannel that has one port on switch 1 and one port on switch 2, each port can receive packets at 29 pps without causing the EtherChannel to become error-disabled.

- 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 switch places the channel (including all physical ports) in the error-disabled state.

- Make sure to limit the rate of ARP packets on incoming trunk ports. Configure higher rates for trunk ports to reflect their aggregation and handle packets across multiple VLANs with Dynamic ARP Inspection enabled. You also can use the **ip arp inspection limit none** 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 Dynamic ARP Inspection (DAI) is enabled 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.

Configure Dynamic ARP Inspection

This section provides information about the various tasks to configure Dynamic ARP Inspection.

Configure ARP ACLs for non-DHCP environments

This procedure shows how to configure Dynamic ARP Inspection when Switch B shown in Figure 2 does not support Dynamic ARP Inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If Host 2's IP address is dynamic, separate Switch A from Switch B at Layer 3 and use a router to route packets between them.

Follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**arp access-list** *acl-name* **Example:** `Device(config)# arp access-list arpacl22`	Defines an ARP ACL, and enters ARP access-list configuration mode. By default, no ARP access lists are defined. **Note** At the end of the ARP access list, there is an implicit **deny ip any mac any** command.
Step 4	**permit ip host** *sender-ip* **mac host** *sender-mac* **Example:** `Device(config-arp-nacl))# permit ip host 10.2.2.2 mac host 0018.bad8.3fbd`	Permits ARP packets from the specified host (Host 2). • For *sender-ip*, enter the IP address of Host 2. • For *sender-mac*, enter the MAC address of Host 2.
Step 5	**exit** **Example:** `Device(config-arp-nacl)# exit`	Exits ARP access-list configuration mode and returns to global configuration mode.
Step 6	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**] **Example:**	Applies ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.

	Command or Action	Purpose
	`Device(config)# ip arp inspection filter arpacl22 vlan 1-2`	• For *arp-acl-name*, specify the name of the ACL created in Step 2. • For *vlan-range*, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) Specify **static** to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used. If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. ARP packets containing only IP-to-MAC address bindings are compared against the ACL. Packets are permitted only if the access list permits them.
Step 7	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitethernt 0/1/1`	Specifies Switch A interface that is connected to Switch B, and enters interface configuration mode.
Step 8	**no ip arp inspection trust** **Example:** `Device(config-if)# no ip arp inspection trust`	Configures Switch A interface that is connected to Switch B as untrusted. By default, all interfaces are untrusted. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.
Step 9	**end** **Example:**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 10	**show arp access-list** *acl-name* **Example:** `Device# show arp access-list arpacl22`	Displays information about the named ACLs.
Step 11	**show ip arp inspection vlan** *vlan-range* **Example:** `Device# show ip arp inspection vlan 1-2`	Displays the statistics for the selected range of VLANs.
Step 12	**show ip arp inspection interfaces** **Example:** `Device# show ip arp inspection interfaces`	Displays the trust state and the rate limit of ARP packets for the provided interface.

Configure Dynamic ARP Inspection in DHCP environments

Before you begin

This procedure shows how to configure Dynamic ARP Inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B. Both switches are running Dynamic ARP Inspection on VLAN 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.

Note Dynamic ARP inspection verifies IP-to-MAC address bindings by relying on entries in the DHCP snooping binding database for incoming ARP requests and ARP responses. Enable DHCP snooping, which permits ARP packets with dynamically assigned IP addresses.

Perform this procedure on both switches to configure Dynamic ARP Inspection.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**show cdp neighbors** **Example:** `Device# show cdp neighbors`	Verify the connection between the switches.

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 4	**ip arp inspection vlan** *vlan-range* **Example:** `Device(config)#` **`ip arp inspection vlan 1`**	Enable Dynamic ARP Inspection on a per-VLAN basis; it is disabled on all VLANs by default. For vlan-range, specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.
Step 5	**Interface** *type number* **Example:** `Device(config)#` **`interface gigabitethernet 1/0/1`**	Specifies the interface connected to the other switch, and enter interface configuration mode.
Step 6	**ip arp inspection trust** **Example:** `Device(config-if)#` **`ip arp inspection trust`**	Configures the connection between the switches as trusted. By default, all interfaces are untrusted. The switch does not check ARP packets that it receives from the other switch on the trusted interface. It simply forwards the packets. For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that intercepted packets have valid IP-to-MAC address bindings before updating the local cache and forwarding the packet to the destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.

Step 7	**end**
	Example:
	`Device(config-if)#` **`end`**
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 8	**show ip arp inspection interfaces** **Example:** `Device#` **`show ip arp inspection interfaces`**	Verifies the Dynamic ARP Inspection configuration on interfaces.

	Command or Action	Purpose
Step 9	**show ip arp inspection vlan** *vlan-range* **Example:** `Device# show ip arp inspection vlan 1`	Verifies the Dynamic ARP Inspection configuration on VLAN.
Step 10	**show ip dhcp snooping binding** **Example:** `Device# show ip dhcp snooping binding`	Verifies the DHCP bindings.
Step 11	**show ip arp inspection statistics vlan** *vlan-range* **Example:** `Device# show ip arp inspection statistics vlan 1`	Checks the Dynamic ARP Inspection statistics on VLAN.

Limit the rate of incoming ARP packets

The switch CPU runs Dynamic ARP Inspection checks. Incoming ARP packets are limited to prevent service disruption.

If incoming ARP packets exceed the limit, the switch disables the port, which remains in that state until error-disabled recovery is enabled so that ports automatically emerge from this state after a specified timeout period.

Note If you do not configure a rate limit, changing the interface's trust state resets its rate limit to the default value. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** interface configuration command, the interface reverts to its default rate limit.

Follow these steps to limit the rate of incoming ARP packets.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)#` **`interface gigabitethernet 0/1/2`**	Specifies the interface to be rate-limited, and enters interface configuration mode.
Step 4	**ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**}	Limits 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 **rate** *pps*, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps. • (Optional) For **burst interval** *seconds*, 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 **rate none**, specify no upper limit for the rate of incoming ARP packets that can be processed.
Step 5	**exit** **Example:** `Device(config-if)#` **`exit`**	Exits interface configuration mode and returns to global configuration mode.
Step 6	Use the following commands: • **errdisable detect cause arp-inspection** • **errdisable recovery cause arp-inspection** • **errdisable recovery interval** *interval* **Example:** `Device(config)#` **`errdisable recovery cause arp-inspection`**	(Optional) Enables error recovery from the Dynamic ARP Inspection error-disabled state, and configures the Dynamic ARP Inspection recover mechanism variables. By default, recovery is disabled, and the recovery interval is 300 seconds. For **interval** *interval*, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.
Step 7	**exit** **Example:** `Device(config)#` **`exit`**	Exits global configuration mode and returns to privileged EXEC mode.

Perform Dynamic ARP Inspection validation checks

Dynamic ARP inspection intercepts and logs ARP packets. It discards packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip arp inspection validate {[src-mac] [dst-mac] [ip]}** **Example:** `Device(config)# ip inspection validate ip`	Performs a specific check on incoming ARP packets. By default, no checks are performed. The keywords have these meanings: • For **src-mac**, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. • For **dst-mac**, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. • For **ip**, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command

	Command or Action	Purpose
		enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip arp inspection vlan** *vlan-range* **Example:** `Device# show ip arp insepction vlan 1-2`	Displays the statistics for the selected range of VLANs.

Configuration examples

In this example, the given ARP ACL is **permit any any**. Any incoming packet is inspected by ARP inspection enabled on VLAN 100 and permitted by this ACL rule. Hence, the ACL permit counter is incremented as shown below (count=1) because of the permit ACL rule hit. If the rule was **deny ip any any**, then the ACL drop counter would have incremented as any incoming packet will hit the deny any rule.

```
Device# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  103     Enabled          Active      dai-2              No

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  103     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  103              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  103              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  103                   0                        0                       0
```

```
Device# show arp access-list

ARP access list dai-2
    permit ip any mac any
```

```
Device# show arp access-list

ARP access list dai-2
    permit ip any mac any

Inspecting pkt from Gi2/0/12
ACL match : NACL Permit
Packet permitted by acl match.intf Gi2/0/12, linktype 1, da 00-00-5E-90-10-01
 Enqueued packet in dai software queuesending packet to PI for processing with SMAC =
00-00-5E-90-10-00{mac} and SRC_ADDR = 10.5.6.7{ipv4}
 0 : sec-cnt : 2, bi : 0, tot : 2
(Gi2/0/12/103)Src: 00-00-5E-90-10-00, Dst: 00-00-5E-90-10-00, SM: 00-00-5E-90-10-00, SI:
10.5.6.7, TM: 00-00-5E-90-10-00, TI: 10.2.3.4
```

```
Device# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  103     Enabled          Active      dai-2              No

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  103     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  103              1              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  103              0              1              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  103                   0                        0                       0
```

This is an example of a case where DHCP packet is permitted. ARP inspection is enabled on the incoming VLAN 100.

The received DHCP packet is forwarded as the programmed DHCP binding table entry contains source MAC address (00-00-5E-90-10-22) that matches the incoming ARP packet's source MAC address (00-00-5E-90-10-22). Hence, ARP inspection forwards the incoming ARP packet and the forward count is reflected under *DHCP Permits*.

```
Device# show ip dhcp snooping bin

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00-00-5E-90-10-22   10.10.10.15      84239       dhcp-snooping  100   GigabitEthernet1/0/4
Total number of bindings: 1
```

```
Device# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  100     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  100     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  100             0               0            0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  100             0             0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  100                   0                        0                       0

Inspecting pkt from Gi1/0/4
 Enqueued packet in dai software queue
 DAI processing: SMAC = 00-00-5E-90-10-22{mac} and SRC_ADDR = 10.10.10.15{ipv4} DMAC =
00-00-5E-90-10-44{mac} and DST_ADDR = 10.10.10.1{ipv4}vlan: 100, if_input: Gi1/0/4
 0 : sec-cnt : 2, bi : 0, tot : 2
 (Gi1/0/4/100)Src: 00-00-5E-90-10-22, Dst: 00-00-5E-90-10-44, SM: 00-00-5E-90-10-22, SI:
10.10.10.15, TM: 00-00-5E-90-10-44, TI: 10.10.10.1

Device# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  100     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  100     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  100             1               0             0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  100             1               0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  100                   0                        0                       0
```

Below is an example of a case where an incoming ARP packet is dropped. ARP inspection is enabled on the incoming VLAN 100.

The received ARP packet is dropped as the programmed DHCP binding table entry contains source MAC address (00-00-5E-90-10-22) that does not match the incoming ARP packet's source MAC address

(00-00-5E-90-10-33). Hence, ARP inspection drops the incoming ARP packet and the drop counter increment is reflected under *DHCP Drops*.

```
Device# show ip dhcp snooping bin

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:00:5E:90:10:22   10.10.10.15      85920       dhcp-snooping  100   GigabitEthernet1/0/4
Total number of bindings: 1

Device# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  100     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  100     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  100             0            0                0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  100             0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  100                   0                        0                       0

Inspecting pkt from Gi1/0/16
Packet marked for log by DHCP bindings.
DHCP snooping binding failure - Dropping packet
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi1/0/16, vlan
100.([00-00-5E-90-10-33/10.10.10.2/00-00-5E-90-10-44/10.10.10.1/01:04:51 UTC Wed Jul 30
2025])

Device# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  100     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  100     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  100             0            1               1             0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
```

```
----   ------------    -----------  -------------   -------------------
 100             0              0             0                     0

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
----   -----------------   ----------------------   ---------------------

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
----   -----------------   ----------------------   ---------------------
 100                   0                        0                       0
```

Monitor Dynamic ARP Inspection

Use these commands to monitor Dynamic ARP Inspection configuration.

Command	Description
clear ip arp inspection statistics	Clears statistics for Dynamic ARP Inspection.
show ip arp inspection	Displays the configuration and the operating state of Dynamic ARP Inspection.
show ip arp inspection statistics [vlan *vlan-range*]	Displays statistics for forwarded packets, dropped packets, MAC validation failures, IP validation failures, ACL permitted and denied packets, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified, or if a range is specified, it displays information only for VLANs with Dynamic ARP Inspection enabled (active).
clear ip arp inspection log	Clears the log buffer for Dynamic ARP Inspection.
show ip arp inspection log	Displays the configuration and contents of the Dynamic ARP Inspection log buffer.
show arp access-list [*acl-name*]	Displays detailed information about ARP ACLs.
show ip arp inspection interfaces [*interface-id*]	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
show ip arp inspection vlan *vlan-range*	Displays the configuration and the operating state of Dynamic ARP Inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with Dynamic ARP Inspection enabled (active).