

Configuring Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on a Cisco NX-OS device.

This chapter includes the following sections:

- About DAI, on page 1
- Prerequisites for DAI, on page 5
- Guidelines and limitations for DAI, on page 5
- Guidelines and limitations for DHCP relay with DAI, on page 6
- Default settings for DAI, on page 6
- Configuring DAI, on page 7
- DAI configuration verification commands, on page 12
- Monitoring and clearing DAI statistics, on page 12
- Configuration examples for DAI, on page 12
- Examples for DHCP relay with DAI, on page 17
- Additional references for DAI, on page 17

About DAI

Explains DAI.

ARP

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. In ARP terms, host B is the sender and host A is the target.

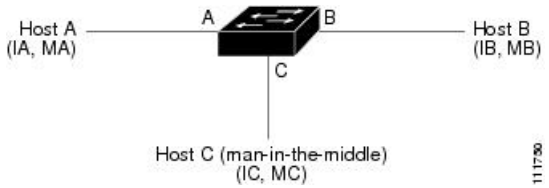
To get the MAC address of host A, host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of host A. All hosts within the broadcast domain receive the ARP request, and host A responds with its MAC address.

ARP spoofing attacks

ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

An ARP spoofing attack can affect hosts, switches, and routers connected to your Layer 2 network by sending false information to the ARP caches of the devices connected to the subnet. Sending false information to an ARP cache is known as ARP cache poisoning. Spoof attacks can also intercept traffic that is intended for other hosts on the subnet.

Figure 1: ARP cache poisoning



Hosts A, B, and C are connected to the device on interfaces A, B, and C, 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 send IP data to host B, it broadcasts an ARP request for the MAC address that is associated with IP address of IB. When host B receives the ARP request, the ARP cache on host B 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 host B responds and the response reaches host A, the ARP cache on host A is populated with an ARP binding for a host with the IP address IB and MAC address MB. The device in between does not populate the ARP cache as both the request and the response are not destined to its local IP address.

Host C can poison the ARP caches of host A and host B by broadcasting two forged ARP responses with bindings: one for a host with the IP address of IA, a MAC address of MC, and another for a host with an IP address of IB and a MAC address of MC. Host B then uses the MAC address MC as the destination MAC address for traffic intended for IA, which means that host C intercepts that traffic. Similarly, host A uses MAC address MC as the destination MAC address for traffic intended for IB.

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. This topology, in which host C has inserted itself into the traffic stream from host A to host B, is an example of a *man-in-the middle* attack.

DAI and ARP spoofing attacks

DAI ensures that only valid ARP requests and responses are relayed. When DAI is enabled and properly configured, a Cisco Nexus device 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

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a Dynamic Host Configuration Protocol (DHCP) snooping binding database. This database can also contain

static entries that you create. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

You can configure DAI 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.

Interface trust states and network security

DAI associates a trust state with each interface on the device. Packets that arrive on trusted interfaces bypass all DAI validation checks, and packets that arrive on untrusted interfaces go through the DAI validation process.

In a typical network configuration, the guidelines for configuring the trust state of interfaces are as follows:

- Untrusted

  Interfaces that are connected to hosts

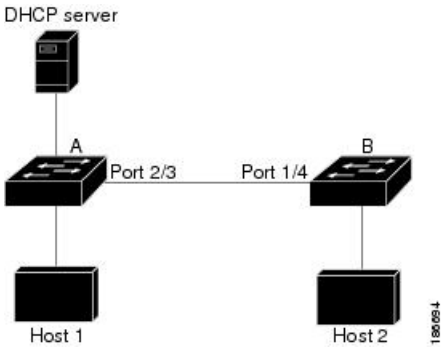
- Trusted

  Interfaces that are connected to devices

With this configuration, all ARP packets that enter the network from a device bypass the security check. No other validation is needed at any other place in the VLAN or in the network.

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

Figure 2: ARP packet validation on a VLAN enabled for DAI



If you configure interfaces as trusted when they should be untrusted, you may open a security hole in a network. If device A is not running DAI, host 1 can easily poison the ARP cache of device B (and host 2, if you configured the link between the devices as trusted). This condition can occur even though device B is running DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a device that runs DAI do not poison the ARP caches of other hosts in the network; however, DAI does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a device that runs DAI.

If some devices in a VLAN run DAI and other devices do not, the guidelines for configuring the trust state of interfaces on a device that runs DAI become the following:

- **Untrusted**

  Interfaces that are connected to hosts or to devices that are not running DAI

- **Trusted**

  Interfaces that are connected to devices that are running DAI

When you cannot determine the bindings of packets from devices that do not run DAI, isolate at Layer 3 the devices that run DAI from devices that do not run DAI.



Note Depending on your network setup, you may not be able to validate a given ARP packet on all devices in the VLAN.

Logging DAI packets

Cisco NX-OS maintains a buffer of log entries about DAI packets processed. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You can also specify the type of packets that are logged. By default, a Cisco Nexus device logs only packets that DAI drops.

If the log buffer overflows, the device overwrites the oldest DAI log entries with newer entries. You can configure the maximum number of entries in the buffer.



Note Cisco NX-OS does not generate system messages about DAI packets that are logged.

DHCP relay with dynamic ARP inspection

DAI uses DHCP snooping client binding database to validate the ARP packets. In releases earlier than Cisco NX-OS Release 10.1(1), this database was built by the DHCP Snooping process, which runs on the switch. The binding database isn't built when the switch acts as a DHCP relay. When snooping, DHCP relay and DAI are enabled together, the relay process takes precedence over snooping for processing incoming DHCP packets. Hence, snooping doesn't build the binding database. Since DAI depends on the binding database, it can't operate with DHCP relay. However, from Cisco NX-OS Release 10.1(1), you can build the binding database using DHCP relay DAI.

When a switch receives a DHCP request, a temporary binding entry is created consisting of the client's MAC address, VLAN, and the incoming interface. After receiving DHCPACK from the server, the binding entry is qualified. The offered IP address is added to the qualified temporary entry and the binding entry type is updated as dhcp-relay.

When you upgrade to Cisco NX-OS Release 10.1(1) or a later release and if you enable this feature, the ISSU proceeds without any error. Disable this feature before you downgrade from Cisco NX-OS Release 10.1(1) to an earlier release.

Prerequisites for DAI

Use this reference to review the prerequisites for DAI.

The prerequisites for DAI are as follows:

- You must enable the DHCP feature before you can configure DAI. See Configuring DHCP.
- You must configure the VLANs on which you want to enable DAI. See the *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*.
- You must configure the ACL TCAM region size for DAI using the **hardware access-list tcam region arp-ether** command. The DAI configuration will not be accepted unless the arp-ether region is effective. See Configure ACL TCAM region sizes.

Guidelines and limitations for DAI

Use this reference to review the guidelines and limitations for DAI.

DAI behavior

DAI has the following configuration guidelines and limitations:

- DAI is an ingress security feature; it does not perform any egress checking.
- DAI is not effective for hosts connected to devices that do not support DAI or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, you should separate the domain with DAI from domains without DAI. This separation secures the ARP caches of hosts in the domain with DAI.

DHCP configuration guidelines

- When you use the **feature dhcp** command to enable the DHCP feature, there is a delay of approximately 30 seconds before the I/O modules receive the DHCP or DAI configuration. This delay occurs regardless of the method that you use to change from a configuration with the DHCP feature disabled to a configuration with the DHCP feature enabled. For example, if you use the rollback feature to revert to a configuration that enables the DHCP feature, the I/O modules receive the DHCP and DAI configuration approximately 30 seconds after you complete the rollback.

Interface and port-channel guidelines

- DAI is supported on access ports, trunk ports, and port-channel ports.
- The DAI trust configuration of a port channel determines the trust state of all physical ports that you assign to the port channel. For example, if you have configured a physical port as a trusted interface and then you add that physical port to a port channel that is an untrusted interface, the physical port becomes untrusted.
- When you remove a physical port from a port channel, the physical port does not retain the DAI trust state configuration of the port channel.

- When you change the trust state on the port channel, the device configures a new trust state on all the physical ports that comprise the channel.

Binding guidelines

- If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, make sure that you have configured the static IP-MAC address bindings.
- ARP ACLs are not supported.
- If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, make sure that DHCP snooping is enabled.

Platform support

Beginning with Cisco NX-OS Release 9.3(3), DAI is supported on Cisco Nexus 9364C-GX, Cisco Nexus 9316D-GX, and Cisco Nexus 93600CD-GX switches.

Guidelines and limitations for DHCP relay with DAI

Use this reference to review the guidelines and limitations for DHCP relay with DAI.

Supported platforms

The following Cisco Nexus platform switches support this feature:

- Cisco Nexus 9300-FX platform switches

Binding database limitations

- The binding database entries are not stored in the hardware.
- The binding database is common for all VRFs. If there are multiple VRFs, map each VRF to a unique VLAN.
- Only IPv4 entries are stored in the binding database. IPv6 is not supported.

Unsupported features

- IP Source Guard (IPSG) does not support this feature.
- This feature does not support vPC.

Default settings for DAI

Use this reference to review the default settings for DAI.

This table lists the default settings for DAI parameters.

Table 1: Default DAI parameters

Parameters	Default
DAI	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
Validation checks	No checks are performed.
Log buffer	When DAI 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.

Configuring DAI

Explains configuring DAI.

Enable or disable DAI on VLANs

You can enable or disable DAI on VLANs. By default, DAI is disabled on all VLANs.

Before you begin

- Make sure that the DHCP feature is enabled.
- Make sure that the VLANs on which you want to enable DAI are configured.
- Make sure that the ACL TCAM region size for DAI (arp-ether) is configured.

Procedure

Step 1 Use the [**no**] **ip arp inspection vlan** *vlan-list* command to enable DAI for the specified list of VLANs. The **no** option disables DAI for the specified VLANs.

Example:

```
switch#configure terminal
switch(config)#ip arp inspection vlan 13
```

Step 2 (Optional) Use the **show ip arp inspection vlan** *vlan-id* command to display the DAI configuration for a specific VLAN.

Example:

```
switch#show ip arp inspection vlan 13
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure the DAI trust state of a layer 2 interface

You can configure the DAI interface trust state of a Layer 2 interface. By default, all interfaces are untrusted.

A device forwards ARP packets that it receives on a trusted Layer 2 interface but does not check them.

On untrusted interfaces, the device intercepts all ARP requests and responses and verifies that the intercepted packets have valid IP-MAC address bindings before updating the local cache and forwarding the packet to the appropriate destination. If the device determines that packets have invalid bindings, it drops the packets and logs them according to the logging configuration.

Before you begin

If you are enabling DAI, make sure that the DHCP feature is enabled.

Procedure

Step 1 Use the **interface** *type port/slot* command to enter interface configuration mode.

Example:

```
switch#configure terminal
switch(config)#interface ethernet 2/1
switch(config-if)#
```

Step 2 Use the [**no**] **ip arp inspection trust** command to configure the interface as a trusted ARP interface. The **no** option configures the interface as an untrusted ARP interface.

Example:

```
switch(config-if)#ip arp inspection trust
```

Step 3 (Optional) Use the **show ip arp inspection interface** *type port/slot* command to display the trust state and the ARP packet rate for the specified interface.

Example:

```
switch#show ip arp inspection interface ethernet 2/1
```

Step 4 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Enable or disable additional validation

You can enable or disable additional validation of ARP packets. By default, no additional validation of ARP packets is enabled. When no additional validation is configured, the source MAC address and the source IP address check against the IP-to-MAC binding entry for ARP packets is performed by using the ARP sender MAC address and the ARP sender IP address.

DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

You can use the following keywords with the **ip arp inspection validate** command to implement additional validations:

- **dst-mac**

  Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

- **ip**

  Checks the ARP body for invalid and unexpected IP addresses. Addresses include 192.0.2.1, 192.0.2.2, 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.

- **src-mac**

  Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling additional validation, follow these guidelines:

- You must specify at least one of the keywords. You can specify one, two, or all three keywords.
- Each **ip arp inspection validate** command that you enter replaces the configuration from any previous commands. If you enter an **ip arp inspection validate** command to enable src-mac and dst-mac validations, and a second **ip arp inspection validate** command to enable ip validation, the src-mac and dst-mac validations are disabled when you enter the second command.

Procedure

Step 1 Use the [**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} command to enable additional DAI validation. The **no** form of this command disables additional DAI validation.

Example:

```
switch#configure terminal
switch(config)#ip arp inspection validate src-mac dst-mac ip
```

Step 2 (Optional) Use the **show running-config dhcp** command to display the DHCP snooping configuration, including the DAI configuration.

Example:

```
switch#show running-config dhcp
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure the DAI logging buffer size

You can configure the DAI logging buffer size. The default buffer size is 32 messages.

Procedure

Step 1 Use the [**no**] **ip arp inspection log-buffer entries** *number* command to configure the DAI logging buffer size. The **no** option reverts to the default buffer size, which is 32 messages. The buffer size can be between 1 and 1024 messages.

Example:

```
switch#configure terminal
switch(config)#ip arp inspection log-buffer entries 64
```

Step 2 (Optional) Use the **show running-config dhcp** command to display the DHCP snooping configuration, including the DAI configuration.

Example:

```
switch#show running-config dhcp
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure DAI log filtering

You can configure how the device determines whether to log a DAI packet. By default, the device logs DAI packets that are dropped.

Procedure

Step 1 Use the [**no**] **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**} command to configure DAI log filtering, as follows. The **no** form of this command removes DAI log filtering.

Example:

```
switch#configure terminal
switch(config)#ip arp inspection vlan 100 dhcp-bindings permit
```

- **all** —Logs all packets that match DHCP bindings.
- **none** —Does not log packets that match DHCP bindings.
- **permit** —Logs packets permitted by DHCP bindings.

Step 2 (Optional) Use the **show running-config dhcp** command to display the DHCP snooping configuration, including the DAI configuration.

Example:

```
switch#show running-config dhcp
```

Step 3 (Optional) Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Enable DHCP relay with DAI

You can create the binding database when DHCP relay and DAI are enabled. This feature is disabled by default.

Before you begin

Enable DAI and DHCP relay. Enable DHCP snooping globally and on VLAN. See the *Configuring DHCP* chapter for more information.

Procedure

Step 1 Use the **ip dhcp relay dai** command to enable creation of binding database in the relay.

Example:

```
switch#configure terminal
switch(config)#ip dhcp relay dai
```

Step 2 (Optional) Use the **show ip dhcp snooping binding relay** command to display the binding entries of the dhcp-relay type.

Example:

```
switch#show ip dhcp snooping binding relay
```

Step 3 (Optional) Use the **show system internal dhcp database global config** command to display if the relay DAI feature is enabled or not.

Example:

```
switch#show system internal dhcp database global config
```

DAI configuration verification commands

Use this reference to verify the DAI configuration.

To display the DAI configuration information, perform one of the following tasks.

Table 2: DAI configuration verification commands

Command	Purpose
show ip arp inspection	Displays the status of DAI.
show ip arp inspection interfaces [**ethernet** *slot/port* | **port-channel** *number*]	Displays the trust state and ARP packet rate for a specific interface or port channel.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection vlan *vlan-id*	Displays the DAI configuration for a specific VLAN.
show running-config dhcp [**all**]	Displays the DAI configuration.

Monitoring and clearing DAI statistics

To monitor and clear DAI statistics, use the commands in this table:

Table 3: Monitoring and clearing DAI statistics

Command	Purpose
show ip arp inspection statistics [**vlan** *vlan-id*]	Displays DAI statistics.
clear ip arp inspection statistics **vlan** *vlan-id*	Clears DAI statistics.
clear ip arp inspection log	Clears DAI logs.

Configuration examples for DAI

Explains configuration examples for DAI.

Two devices support DAI

These procedures show how to configure DAI when two devices support DAI.

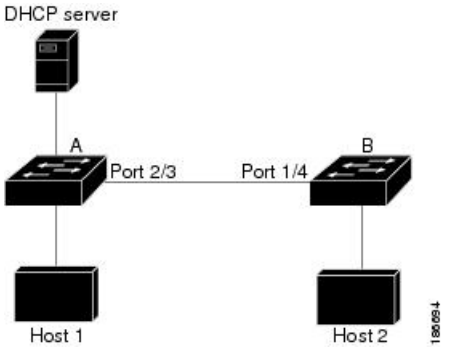
DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically-assigned IP addresses.

- This configuration does not work if the DHCP server is moved from device A to a different location.

- To ensure that this configuration does not compromise security, configure Ethernet interface 2/3 on device A and Ethernet interface 1/4 on device B as trusted.

The following figure shows the network configuration for this example. Host 1 is connected to device A, and Host 2 is connected to device B. Both devices are running DAI on VLAN 1 where the hosts are located. A DHCP server is connected to device A. Both hosts acquire their IP addresses from the same DHCP server. Device A has the bindings for Host 1 and Host 2, and device B has the binding for Host 2. Device A Ethernet interface 2/3 is connected to device B Ethernet interface 1/4.

Figure 3: Two devices supporting DAI



Configure device a

To enable DAI and configure Ethernet interface 2/3 on device A as trusted, follow these steps:

Procedure

Step 1 While logged into device A, verify the connection between device A and device B.

```
switchA#show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I       WS-C2960-24TC Ethernet1/4
switchA#
```

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

```
switchA#configure terminal
switchA(config)#ip arp inspection vlan 1
switchA#show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

Step 3 Configure Ethernet interface 2/3 as trusted.

```
switchA(config)#interface ethernet 2/3
switchA(config-if)#ip arp inspection trust
switchA(config-if)#exit
switchA(config)#exit
switchA#show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/3      Trusted           15             5
```

Step 4 Verify the bindings.

```
switchA#show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:00:5E:00:53:01  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
switchA#
```

Step 5 Check the statistics before and after DAI processes any packets.

```
switchA#show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

If host 1 sends out two ARP requests with an IP address of 10.0.0.1 and a MAC address of 0002.0002.0002, both requests are permitted and are shown as follows:

```
switchA#show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

If host 1 tries to send an ARP request with an IP address of 10.0.0.3, the packet is dropped, and an error message is logged.

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/192.0.2.1/02:42:35 UTC Fri Jan 23 2015])
```

The statistics display as follows:

```
switchA#show ip arp inspection statistics vlan 1
switchA#Vlan : 1
-----------
ARP Req Forwarded  = 2
```

```
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

Configure device b

To enable DAI and configure Ethernet interface 1/4 on device B as trusted, follow these steps:

Procedure

Step 1 While logged into device B, verify the connection between device B and device A.

```
switchB#show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID             Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA               Ethernet1/4     120     R S I       WS-C2960-24TC Ethernet2/3
switchB#
```

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

```
switchB#configure terminal
switchB(config)#ip arp inspection vlan 1
switchB#show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchB(config)#
```

Step 3 Configure Ethernet interface 1/4 as trusted.

```
switchB(config)#interface ethernet 1/4
switchB(config-if)#ip arp inspection trust
switchB(config-if)#exit
switchB(config)#exit
switchB#show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15             5
switchB#
```

Step 4 Verify the list of DHCP snooping bindings.

```
switchB#show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:00:5E:00:53:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

Step 5 Check the statistics before and after DAI processes any packets.

```
switchB#show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

If Host 2 sends out an ARP request with the IP address 10.0.0.2 and the MAC address 0001.0001.0001, the packet is forwarded, and the statistics are updated.

```
switchB#show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

If Host 2 attempts to send an ARP request with the IP address 10.0.0.1, DAI drops the request and logs the following system message:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/192.0.2.1/01:53:21 UTC Fri Jan 23 2015])
```

The statistics display as follows:

```
switchB#show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
```

```
IP Fails-ARP Res   = 0
switchB#
```

Examples for DHCP relay with DAI

Use this reference to review examples for DHCP relay with DAI.

DHCP relay DAI status example

The following example displays whether the DHCP relay DAI feature is enabled. If the feature is not enabled, the value of the *DHCP Relay DAI enabled* entry in the database is *No*.

```
switch# show system internal dhcp database global config
Snooping enabled: Yes
Snoop option-82 enabled: No
Relay enabled: Yes
.
.
DHCP Relay DAI enabled : No
Validate source mac: No
Validate destination mac: No
```

Additional references for DAI

Use this reference to find additional references for DAI.

Related documents

Use this reference to review related documents.

Related documents

Table 4: Related documents

Related Topic	Document Title
ACL TCAM regions	Configure IP ACLs
DHCP and DHCP snooping	Configuring DHCP

Standards

Use this reference to review standards.

Table 5: Standards:

Standard	Title	
RFC-826	An Ethernet Address Resolution Protocol (https://example.com/doc/html/rfc826)	