Configuring Dynamic ARP Inspection

This chapter contains the following sections:

Information About Dynamic ARP Inspection

This section provides information about DAI features.

ARP

Dynamic ARP Inspection (DAI) ensures that only valid ARP requests and responses are relayed by intercepting all ARP requests and responses on untrusted ports and verifying 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. When this feature is enabled, invalid ARP packets are dropped.

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.

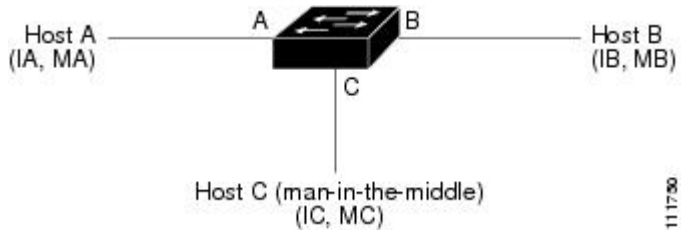
Starting with Release 4.2(1)SV2(1.1), you can filter the traffic based on the source IP address only as opposed to filtering the traffic based on the IP-MAC Address pair. For more information, refer to Enabling Source IP-Based Filtering, on page 14.

ARP Spoofing Attacks

In an ARP spoofing attack, a host allows an unsolicited ARP response to update its cache so that traffic is directed through the attacker until it is discovered and the information in the ARP cache is corrected.

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.

Figure 1: ARP Cache Poisoning



In the figure, hosts A, B, and C are connected to the device 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 send IP data to host B, it broadcasts an ARP request for the MAC address associated with IP address IB. When the device and host B receive the ARP request, they add a binding to their ARP caches for a host with the IP address IA and a MAC address MA.

When host B responds, the device and host A update their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can spoof host A and B by broadcasting the following forged ARP responses:

- One for Host B with an sorce IP Address IA and source MAC address MC
- One for Host A with an source IP Address IB and source MAC address MC

Host B then uses MC as the destination MAC address for traffic that was intended for IA, which means that host C intercepts that traffic. Likewise, host A uses MC as 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

DAI is used to validate ARP requests and responses as follows:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet.
- 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 is built by DHCP snooping when it is enabled on the VLANs and on the device. It may also contain static entries that you have created.

If an 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 and Network Security

DAI identifies interfaces as trusted or untrusted.

In a typical network, interfaces are configured as follows:

- Untrusted—Interfaces that are connected to hosts.

  Packets are validated by DAI.

- Trusted—Interfaces that are connected to devices.

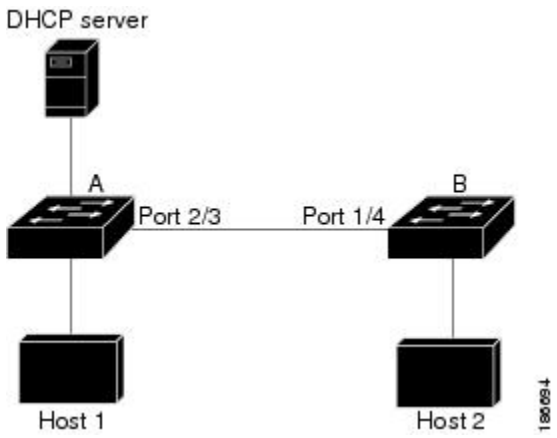
  Packets bypass all DAI validation checks.

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.

In the following figure, assume that both device A and device B are running DAI 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 device A, only device A binds the IP-to-MAC address of host 1. If the interface between device A and device B is untrusted, the ARP packets from host 1 are dropped by device B and connectivity between host 1 and host 2 is lost.

Figure 2: ARP Packet Validation on a VLAN Enabled for DAI



If you configure interfaces as trusted when they should be untrusted, you might 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.

Prerequisites for DAI

- You must be familiar with the following:
  - ARP
  - DHCP snooping
- The software running on your Cisco Nexus 1000V must support DAI.
- The VEM feature level must be updated to a release that supports DAI.

Guidelines and Limitations for DAI

- DAI is an ingress security feature and does not perform any egress checking.
- DAI is not effective when the host is connected to a device that does not support DAI or that does not have DAI enabled. To prevent attacks that are limited to a single Layer 2 broadcast domain, you should separate a domain with DAI from those domains without DAI. This separation secures the ARP caches of hosts in the domain with 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. If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, you must configure DHCP snooping only. If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, you must configure DHCP snooping on the same VLANs on which you configure DAI.
- DAI is supported on vEthernet interfaces and private VLAN ports
- Virtual Service Domain (VSD) service VM ports are trusted ports by default. Even if you configure VSD ports as untrusted, they still appear as trusted ports to DAI.

Default Settings for DAI

Parameters	Default
VLAN	VLANs are not configured for DAI.
Trust state of vEthernet interfaces not in a VSD	Untrusted.

Parameters	Default
Trust state of vEthernet interfaces in a VSD	Trusted.
Trust state of Ethernet port channels	Trusted.
Incoming ARP packet rate limit for untrusted interfaces	15 packets per second (pps).
Incoming ARP packet rate limit for trusted	15 packets per second (pps).
Rate limit burst interval	5 seconds.
Detecting and recovering DAI error-disabled interfaces	Error-disabled detection and recovery is not configured.
Validation checks (source MAC/ Destination MAC /IP)	No checks are performed.
VLAN statistics	ARP request and response statistics.

Configuring DAI Functionality

Configuring a VLAN for DAI

By default, VLANs are not configured for DAI.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable DHCP snooping.
- Create the VLANs that you want to configure for DAI.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ip arp inspection vlan** *list*	Configures the specified VLAN or list of VLANs for DAI.
Step 3	(Optional) switch(config)# **show ip arp inspection vlan** *list*	Displays the DAI status for the specified list of VLANs.
Step 4	switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure a VLAN for DAI:

```
switch# configure terminal
switch(config)# ip arp inspection vlan 100
switch(config)# show ip arp inspection vlan 100
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled

Filter Mode (for static bindings): IP-MAC

Vlan : 100
-----------
Configuration : Enabled
Operation State : Active
DHCP logging options : Deny
switch(config)# copy running-config startup-config
```

Configuring a Trusted vEthernet Interface

By default, vEthernet interfaces are untrusted, unless they are part of a VSD.

If an interface is untrusted, all ARP requests and responses are verified for a valid IP-MAC address binding before the local cache is updated and the packet forwarded. If a packet has an invalid IP-MAC address binding, it is dropped.

ARP packets that are received on a trusted interface are forwarded but not checked.

You can configure a trusted interface on either of the following:

- The interface itself
- The existing port profile that the interface is assigned to

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in interface configuration mode for the specified vEthernet interface.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile.
Step 4	switch(config-if)# [**no**]**ip arp inspection trust**	The **no** option configures the port as untrusted for ARP inspection.

	Command or Action	Purpose
Step 5	switch(config-port-profile)# **ip arp inspection trust**	Configures the interfaces assigned to the port profile as trusted ARP interfaces.
Step 6	(Optional) switch(config-if)# **show ip arp inspection interface vethernet** *interface-number*	Displays the trusted state and the ARP packet rate for the specified interface.
Step 7	(Optional) switch(config-if)# **show port-profile name** *profilename*	Displays the port profile configuration including the ARP trusted state.
Step 8	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure a trusted vEthernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip arp inspection trust
switch(config-if)# show ip arp inspection interfaces vethernet 3

Interface Trust State Pkt Limit Burst Interval
------------- ----------- --------- --------------
Vethernet3 Trusted 0 0
switch(config-if)# copy running-config startup-config

switch(config-if)# port-profile vm-data
switch(config-port-prof)# ip arp inspection trust
switch(config-port-prof)# show port-profile name vm-data

port-profile vm-data
type: Vethernet
description:
status: enabled
max-ports: 32
min-ports: 1
inherit:
config attributes:
switchport mode access
switchport access vlan 100
ip arp inspection trust
no shutdown
evaluated config attributes:
switchport mode access
switchport access vlan 100
ip arp inspection trust
no shutdown
assigned interfaces:
port-group: vm-data
system vlans: none
capability l3control: no
capability iscsi-multipath: no
capability vxlan: no
capability l3-vservice: no
port-profile role: none
port-binding: static
```

```
switch(config-port-prof)# copy running-config startup-config
```

Resetting a vEthernet Interface to Untrusted

By default, vEthernet interfaces are untrusted, unless they are part of a VSD. You can remove a trusted designation from a vEthernet interface and return it to the default untrusted designation.

If an interface is untrusted, all ARP requests and responses are verified for a valid IP-MAC address binding before the local cache is updated and the packet forwarded. If a packet has an invalid IP-MAC address binding, it is dropped.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in the interface configuration mode for the specified vEthernet interface.
Step 3	switch(config-if)# **default ip arp inspection trust**	Removes the trusted designation from the interface and returns it to the default untrusted state.
Step 4	(Optional) switch(config-if)# **show ip arp inspection interface vethernet** *interface-number*	Displays the trusted state and the ARP packet rate for the specified interface.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to reset a vEthernet interface to a untrusted state:

```
switch(config-if)# default ip arp inspection trust
switch(config-if)# show ip arp inspection interface vethernet 3
Interface     Trust State Pkt Limit Burst Interval
------------- ----------- --------- ----------------
Vethernet3     Untrusted   15          5
switch(config-if)# copy running-config startup-config
```

Configuring DAI Rate Limits

You can set the rate limit of ARP requests and responses.

Because of their aggregation, trunk ports should be configured with higher rate limits.

Once the rate of incoming packets exceeds the configured rate, the interface is automatically put into an errdisable state.

The default DAI rate limits are as follows:

- Untrusted interfaces—15 packets per second
- Trusted interfaces—Unlimited
- Burst interval—5 seconds

You can configure the rate limits for an interface on either of the following:

- The interface itself
- The existing port profile that the interface is assigned to
- If configuring the port profile, it has already been created and you know its name.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in interface configuration mode for the specified vEthernet interface.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile.

Step 4	switch(config-if)# **ip arp inspection limit** {**rate** *pps* [**burst interval** l *bint*] | **none**}	Configures the specified ARP inspection limit on the interface or the port profile as follows.
		The keywords are as follows:
		• **rate**—Specifies that allowable values are between 1 and 2048 packets per second (pps).
		  • The untrusted interface default is15 packets per second.
		  • The trusted interface default is15 packets per second.
		• **burst interval**—Specifies that allowable values are between 1 and 15 seconds (the default is 5 seconds).
		• **none**—Specifies an unlimited number of packets per second.

	Command or Action	Purpose
Step 5	(Optional) switch(config-if)# **show ip arp inspection interface vethernet interface-number**	Displays the trusted state and the ARP packet rate for the specified interface.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to create DAI rate limits:

```
switch# configure terminal
switch(config)#interface vethernet 3
switch(config-if)#ip arp inspection limit rate 30
switch# show ip arp inspection interfaces vethernet 3

Interface Trust State Pkt Limit Burst Interval
------------- ----------- --------- -----------------
Vethernet9 Untrusted    30          5
switch#copy running-config startup-config
```

Resetting DAI Rate Limits to Default Values

You can set the rate limit of ARP requests and responses.

Because of their aggregation, trunk ports should be configured with higher rate limits.

Once the rate of incoming packets exceeds the configured rate, the interface is automatically put into an errdisable state.

The default DAI rate limits are as follows:

- Untrusted interfaces—15 packets per second
- Trusted interfaces—Unlimited
- Burst interval—5 seconds

You can configure the rate limits for an interface on either of the following:

- The interface itself
- The existing port profile that the interface is assigned to

  If configuring the port profile, it has already been created and you know its name.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in interface configuration mode for the specified vEthernet interface.

Step 3	switch(config-if)# **default ip arp inspection limit** {**rate** *pps* [**burst interval**l *bint*] | **none**}	Removes the configured DAI rate limits from the interface and returns them to the default values.
		The keywords are as follows:
		• **rate**—Specifies that the untrusted interface default is 15 packets per second.
		  • The untrusted interface default is 15 packets per second.
		  • The trusted interface default is 15 packets per second.
		• **burst interval**—Specifies the range is from 1 to 15 seconds. The default is 5 seconds.
		• **none**—Specifies an unlimited number of packets per second.

Step 4	(Optional) switch(config)# **show ip arp inspection interface vethernet** *interface-number*	Displays the default ARP packet rate for the specified interface.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to reset DAI rate limits to their default values:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# default ip arp inspection limit rate

switch# show ip arp inspection interface vethernet 3
<------no output expected for this, since interface moved to default---->

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

Detecting and Recovering Error-Disabled Interfaces

By default, interfaces are not configured for DAI error-disabled recovery.

To manually recover an interface from the error-disabled state, use the following command sequence.

1. **shutdown**
2. **no shutdown**

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **errdisable detect cause arp-inspection**	Configures the detection of interfaces that have been error-disabled by ARP inspection. The **no** option disables the detection.
Step 3	switch(config)# [**no**] **errdisable recovery cause arp-inspection**	Configures the auto-recovery of interfaces that have been error-disabled by ARP inspection.
Step 4	switch(config)# **errdisable recovery interval** *timer-interval*	Configures the recovery interval for interfaces that have been error-disabled by ARP inspection. The *timer-interval* is from 30 to 65535 seconds.
Step 5	(Optional) switch(config)# **show errdisable detect**	Displays the errdisable configuration.
Step 6	(Optional) switch(config)# **show errdisable recovery**	Displays the errdisable configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to detect and recover error-disabled interfaces:

```
switch# configure terminal
switch(config)# errdisable detect cause arp-inspection
switch(config)# errdisable recovery cause arp-inspection
switch(config)# errdisable recovery interval 30
switch(config)# show errdisable detect
ErrDisable Reason Timer Status
----------------- ------------
link-flap enabled
bpduguard enabled
dhcp-rate-limit enabled
```

```
arp-inspection enabled
ip-addr-conflict enabled
switch(config)# show errdisable recovery
ErrDisable Reason Timer Status
----------------- ------------
link-flap disabled
bpduguard disabled
dhcp-rate-limit enabled
arp-inspection enabled
security-violation disabled
psecure-violation enabled
failed-port-state enabled
ip-addr-conflict disabled

Timer interval: 30
switch(config)# copy running-config startup-config
```

Validating ARP Packets

You can enable validation of the following, which are disabled by default:

- Destination MAC address

  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 address

  Checks the ARP body for invalid and unexpected IP addresses, including 0.0.0.0, 255.255.255.255, and any IP multicast address. Sender IP addresses are checked in both ARP requests and responses. Target IP addresses are checked only in ARP responses.

- Source MAC address

  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.

Note Whenever you configure a validation, any previous validation configuration is overwritten.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# [**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}	Enables the specified validation and overwrites any existing validation that was previously saved: • Source MAC • Destination MAC • IP You can specify all three of these validations but you must specify at least one. Use the **no** option to disable a validation.
Step 3	(Optional) switch(config)# **show ip arp inspection**	Displays the DAI configuration.
Step 4	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to validate ARP packets:

```
switch# configure terminal
switch(config)# ip arp inspection
switch(config)# show ip arp inspection
Source Mac Validation      : Enabled
Destination Mac Validation      : Enabled
IP Address Validation      : Enabled

Filter Mode(for static bindings): IP-MAC
switch(config)# copy running-config startup-config
```

Enabling Source IP-Based Filtering

When you assign static IP addresses to virtual machines (VMs) in the deployment and the VMs power on and off frequently, the MAC addresses of the VMs change. This situation affects the Dynamic ARP Inspection (DAI) and the IP Source Guard (IPSG) functionality on the Cisco Nexus 1000V. The Cisco Nexus 1000V does not have the same IP-MAC address binding. Therefore, the traffic from these VMs is dropped.

Starting with Release 4.2(1)SV2(1.1), you can filter the traffic based on the source IP address only. The Cisco Nexus 1000V ignores the MAC address and validates only the source IP address of the traffic from the VMs. This new functionality is applicable to static bindings only.

To enable source IP based filtering on the Cisco Nexus 1000V switch, set the filter mode to ip filtering. The default filtering mode is the ip-mac filtering mode.

Before you begin

- Log in to the CLI in EXEC mode.

- Enable DHCP feature on the Cisco Nexus 1000V switch.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enables DHCP globally. DHCP snooping is available as an advanced feature that requires a license.
Step 3	switch(config)# **ip source binding filter-mode ip | ip-mac**	Configures the filter mode.
Step 4	(Optional) switch(config)# **show ip source binding filter-mode**	Displays the filter mode on the switch.
Step 5	(Optional) switch(config)# **show ip arp inspection**	Displays the filter mode as part of the output.
Step 6	(Optional) switch(config)# **show ip arp inspection vlan***vlan-id*	Displays the filter mode as part of the output.
Step 7	(Optional) switch(config)# **show ip verify source**	Displays the filter mode as part of the output.
Step 8	(Optional) switch(config)# **show ip verify source interface vethernet** *interface-number*	Displays the filter mode as part of the output.

Example

This example shows how to filter the traffic based on the **IP** filter mode:

```
switch# configure terminal
switch(config)# feature dhcp
switch# show ip source binding filter-mode
DHCP Snoop Filter Mode(for static bindings) = IP-MAC
switch# configure terminal
switch(config)# ip source binding filter-mode ip
switch# show ip source binding filter-mode
DHCP Snoop Filter Mode(for static bindings) = IP
switch# show ip arp inspection

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

Filter Mode(for static bindings): IP

Vlan : 1
-----------
Configuration          : Enabled
Operation State        : Active
DHCP logging options   : Deny

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

switch# show ip verify source
Filter Mode(for static bindings): IP
IP source guard is enabled on the following interfaces:
-------------------------------------------------------
        Vethernet1
        Vethernet2
        Vethernet3
        Vethernet4
        Vethernet5
        Vethernet6
        Vethernet7
        Vethernet8
        Vethernet9
        Vethernet10


IP source guard operational entries:
------------------------------------
Interface         Filter-mode             IP-address     Mac-address       Vlan
------------      -----------             ----------     --------------    ----
Vethernet1        active                1.182.56.137   00:50:56:82:56:3e  1
Vethernet2        active                1.182.56.138   00:50:56:82:56:3f  1
Vethernet3        active                1.182.56.139   00:50:56:82:56:40  1
Vethernet4        active                1.182.56.140   00:50:56:82:56:41  1
Vethernet5        active                1.182.56.141   00:50:56:82:56:42  1
Vethernet6        active                1.182.56.142   00:50:56:82:56:43  1
Vethernet7        active                1.182.56.143   00:50:56:82:56:44  1
Vethernet8        active                1.182.56.144   00:50:56:82:56:45  1
Vethernet9        active                1.182.56.145   00:50:56:82:56:46  1
Vethernet10       active                1.182.56.146   00:50:56:82:56:47  1
switch#

switch# show ip verify source interface vethernet 1
Filter Mode(for static bindings): IP
IP source guard is  enabled on this interface.

Interface         Filter-mode             IP-address     Mac-address       Vlan
------------      -----------             ----------     --------------    ----
Vethernet1        active                1.182.56.137   00:50:56:82:56:3e    1
```

Verifying the DAI Configuration

Use the following commands to verify the configuration:

Command	Purpose
show running-config dhcp	Displays the DAI configuration.
show ip arp inspection	Displays the status of DAI.

Command	Purpose
show ip arp inspection interface vethernet *interface-number*	Displays the trust state and ARP packet rate for a specific interface.
show ip arp inspection vlan *vlan-ID*	Displays the DAI configuration for a specific VLAN.

Monitoring DAI

Use the following commands to monitor DAI:

Command	Purpose
show ip arp inspection statistics	Displays DAI statistics.
show ip arp inspection statistics vlan *vlan-ID*	Displays DAI statistics for a specified VLAN.
clear ip arp inspection statistics	Clears DAI statistics.

This example shows how to display IP ARP statistics:

```
switch# show ip arp inspection statistics

Vlan : 13
-----------
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

Vlan : 1054
-----------
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

Vlan : 1058
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
```

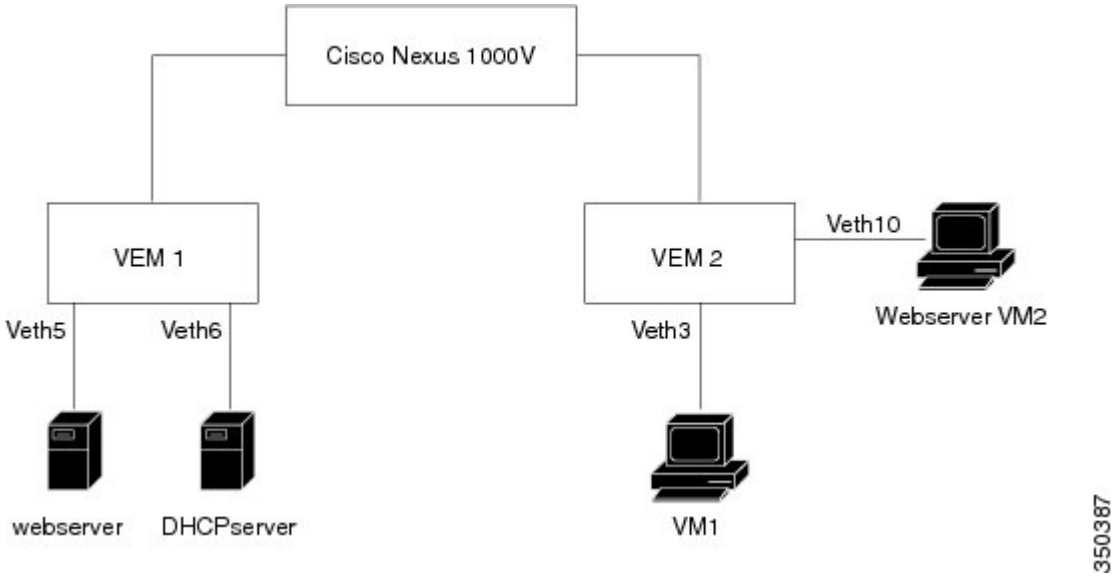
```
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0


switch# show ip arp inspection statistics vlan 13

Vlan : 13
-----------
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
switch#
```

Configuration Examples for DAI

These examples show how to configure DAI in a network with two VEMs:

- One VEM is hosting an authentic web server and a DHCP server.
- The other VEM is hosting a client Virtual Machine (VM 1) and a Virtual Machine (VM 2) with a rogue web server. VM 1 is connected to vEthernet interface 3, which is untrusted by default, and belongs to VLAN 1. VM 2 is connected to vEthernet 10 and VLAN 1.

Figure 3: Configuring DAI in a Network



Without DAI enabled, VM 2 can spoof the ARP cache in VM 1 by sending a packet even though an ARP request was not generated. In this case, the packet directs VM 1 to send its traffic to the VM 2 web server instead of the authentic web server.

If DAI is enabled when VM2 attempts to spoof the ARP cache in VM1, the unsolicited ARP packet sent by VM 2 is dropped because DAI detects the invalid IP-to-MAC address binding. The attempt to spoof the ARP cache fails, and VM 1 connects to the authentic web server.

Note DAI depends on the DHCP snooping 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.

Enabling DAI on VLAN 1 and Verifying the Configuration

This example shows how to enable DAI on VLAN 1 and add a static binding for the web server on interface veth5:

```
switch# configure terminal
switch(config)# feature dhcp

switch(config)# ip arp inspection vlan 1

switch# show ip arp inspection vlan 1

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

Filter Mode (for static bindings): IP-MAC

Vlan : 1
-----------
Configuration        : Enabled
Operation State      : Active
DHCP logging options : Deny

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

Note: Validate helps in inspecting the dst-mac,src-mac and ip of ARP packet and Ethernet
Header, while sending the ARP packet.

switch(config)# ip source binding 192.168.2.22 00:50:56:1e:2c:1c vlan 1 interface vethernet
 5
switch# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type        VLAN  Interface
-----------------  ---------------  --------  ----------  ----  -------------
00:50:56:1e:2c:1c  22.22.22.23      infinite   static      1     Vethernet5

switch(config)# int vethernet 6
switch(config-if)# ip arp inspection trust

switch# show ip arp inspection interfaces vethernet 6
Interface Trust State Pkt Limit Burst Interval
------------- ----------- --------- -----------------
Vethernet6 Trusted 0 0
```

```
switch(config)# interface vethernet 3
switch(config-if)# ip arp inspection limit rate 20
switch# show ip arp inspection interfaces vethernet 3

 Interface        Trust State        Pkt Limit      Burst Interval
 -------------    -----------        ---------      ----------------
 Vethernet3          Untrusted           20               5

switch(config)# errdisable detect cause arp-inspection

switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  -------------
00:50:56:1e:2c:1c  192.168.2.22     infinite   static       1     Vethernet5
00:50:56:82:56:43  192.168.2.2      infinite   static       1     Vethernet6
00:50:56:82:56:3e  192.168.2.11     9000       dhcp-snoop   1     Vethernet1
00:50:56:82:56:3f  192.168.2.12     9000       dhcp-snoop   1     Vethernet3
00:50:56:82:56:40  192.168.2.13     9000       dhcp-snoop   1     Vethernet10


If the Rouge-server sends an ARP packet with an IP of 192.168.2.22 (IP of the webserver)
and a MAC address of 00:50:56:82:56:40, ARP packet will be
dropped. An error message will be logged as shown below:

2013 Mar  6 03:54:04 switch %DHCP_SNOOP-SLOT130-3-DHCPDENIEDARP: ARP frame denied due to
DHCP snooping binding on interface Veth10 vlan 1 sender
mac 00:50:56:82:56:40 sender ip 192.168.2.22 target mac 00:50:56:82:56:3f target ip
192.168.2.12.

If Veth3 send ARP packets greater than the configured limit, Veth3 will be placed into error
 disabled state with the following message.
2013 Mar  6 05:26:22 switch %DHCP_SNOOP-4-ERROR_DISABLED: Interface Vethernet3 has moved
to error disabled state due to excessive rate 20 of
ingress ARP packets
```

Example of Displaying the Statistics for DAI

This example shows how to display the statistics for DAI:

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

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
switch#
```

Standards

Standards	Title
RFC-826	An Ethernet Address Resolution Protocol http://tools.ietf.org/html/rfc826

Feature History for DAI

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
Licensing changes	4.2(1)SV2(1.1)	DAI is available as an advanced feature. Use the **feature dhcp** command to enable the feature.
Enabling source IP-based filtering	4.2(1)SV2(1.1)	You can enable source IP-based filtering on the Cisco Nexus 1000V switch.
DAI	4.0(4)SV1(2)	This feature was introduced.