



Configuring Dynamic ARP Inspection

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



Note

The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter includes the following sections:

- [Information About DAI, page 2](#)
- [Licensing Requirements for DAI, page 5](#)
- [Prerequisites for DAI, page 6](#)
- [Platform Support for DAI and ARP ACLs, page 6](#)
- [Configuring DAI, page 6](#)
- [Monitoring and Clearing DAI Statistics, page 11](#)
- [Field Descriptions for DAI, page 11](#)
- [Configuring ARP ACLs, page 13](#)
- [Field Descriptions for ARP ACLs, page 15](#)
- [Additional References for DAI, page 19](#)
- [Feature History for DAI, page 19](#)

Information About DAI

Understanding 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.

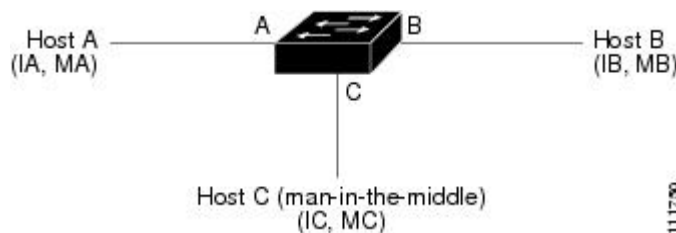
Understanding ARP Spoofing Attacks

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

Understanding 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 NX-OS 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 is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. It 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.

DAI can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. The device logs dropped packets.

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.

Related Topics

- [Applying ARP ACLs to VLANs for DAI Filtering](#), page 8
- [Logging DAI Packets](#), page 5
- [Enabling or Disabling Additional Validation](#), page 9

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.

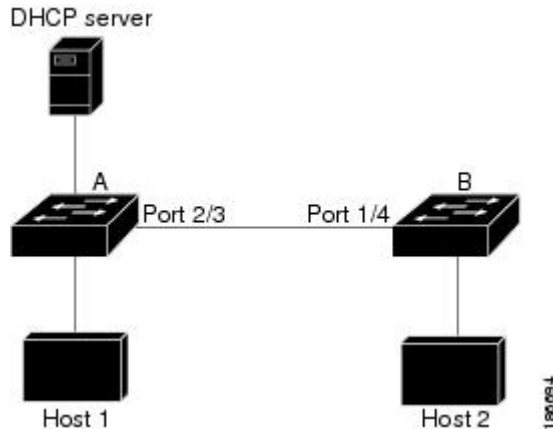


Caution

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

In this 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 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, then the guidelines for configuring the trust state of interfaces on a device running DAI becomes the following:

Untrusted	Interfaces that are connected to hosts or to devices that <i>are not</i> running DAI
Trusted	Interfaces that are connected to devices that <i>are</i> running DAI

To validate the bindings of packets from devices that are not running DAI, configure ARP ACLs on the device running DAI. When you cannot determine the bindings, 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.

Related Topics

- [Configuring the DAI Trust State of a Layer 2 Interface](#) , page 7

Prioritizing ARP ACLs and DHCP Snooping Entries

By default, DAI filters DAI traffic by comparing DAI packets to IP-MAC address bindings in the DHCP snooping database.

When you apply an ARP ACL to traffic, the ARP ACLs take precedence over the default filtering behavior. The device first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the device denies the packet regardless of whether a valid IP-MAC binding exists in the DHCP snooping database.



Note

VLAN ACLs (VACLs) take precedence over both ARP ACLs and DHCP snooping entries. For example, if you apply a VACL and an ARP ACL to a VLAN and you configured the VACL to act on ARP traffic, the device permits or denies ARP traffic as determined by the VACL, not the ARP ACL or DHCP snooping entries.

Related Topics

- [Configuring ARP ACLs, page 13](#)
- [Applying ARP ACLs to VLANs for DAI Filtering, page 8](#)

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 NX-OS 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.

Related Topics

- [Configuring the DAI Logging Buffer Size, page 9](#)
- [Configuring DAI Log Filtering, page 10](#)

Licensing Requirements for DAI

This table shows the licensing requirements for DAI.

Product	License Requirement
Cisco DCNM	DAI requires a LAN Enterprise license. For an explanation of the Cisco DCNM licensing scheme

Product	License Requirement
	and how to obtain and apply licenses, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	DAI requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites for DAI

The following prerequisites are required for using this feature on Cisco DCNM. For a full list of feature-specific prerequisites, see the platform-specific documentation.

- System-message logging levels for the DAI feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the .

Platform Support for DAI and ARP ACLs

The following platform supports these features. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Configuring DAI

Enabling or Disabling DAI on VLANs

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

Before You Begin

If you are enabling DAI, ensure the following:

- The VLANs on which you want to enable DAI are configured.

Procedure

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
 - Step 2** From the Summary pane, double-click the device that has the VLAN that you want to configure with DAI. The VLANs on the device appear in the Summary pane.
 - Step 3** From the Summary pane, click the VLAN that you want to configure with DAI. The DAI VLAN Details tab appears in the Details pane.
 - Step 4** From the DAI VLAN Details tab, do one of the following:
 - To enable DAI on the selected VLAN, check **ARP Inspection**.
 - To disable DAI on the selected VLAN, uncheck **ARP Inspection**.
 - Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring 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 verifies that all ARP requests and ARP responses 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.

Procedure

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, click the device that has the Layer 2 interface whose DAI trust state you want to configure. The Details tab appears in the Summary pane.
- Step 3** From the Details tab, expand the **ARP Trust State** section, if necessary. A table of slots on the selected device appears in the ARP Trust State section.
- Step 4** Double-click the slot that contains the Layer 2 interface that you want to configure. The Layer 2 interfaces on the slot appear. For each interface, a check box in the Trust State column indicates whether the device trusts the interface.
- Step 5** In the Trust State column for the interface that you want to configure, do one of the following:
 - To make the interface a trusted DAI interface, check **Trust State**.

- To make the interface an untrusted DAI interface, uncheck **Trust State**.

Step 6 From the menu bar, choose **File** ► **Deploy** to apply your changes to the device.

Related Topics

- [Interface Trust States and Network Security, page 3](#)
- [Configuring DAI Log Filtering, page 10](#)

Applying ARP ACLs to VLANs for DAI Filtering

You can apply an ARP ACL to one or more VLANs. The device permits packets only if the ACL permits them. By default, no VLANs have an ARP ACL applied.

Before You Begin

Ensure that the ARP ACL that you want to apply is correctly configured.

Procedure

- Step 1** From the Feature Selector pane, choose **Switching** ► **Layer 2 Security** ► **ARP Inspection**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that has the VLAN that you want to configure with an ARP ACL. The VLANs on the device appear in the Summary pane.
- Step 3** From the Summary pane, click the VLAN that you want to configure with an ARP ACL. The DAI VLAN Details tab appears in the Details pane. On the DAI VLAN Details tab, the ARP ACL drop-down list appears.
- Step 4** From the DAI VLAN Details tab, do one of the following:
- To add an ARP ACL to the VLAN, from the ARP ACL drop-down list, choose the ACL that you want to apply.
 - To remove an ARP ACL from the VLAN, from the menu bar, choose **Actions** ► **Remove ARP ACL from VLAN**.
- Step 5** From the menu bar, choose **File** ► **Deploy** to apply your changes to the device.
-

Related Topics

- [Configuring ARP ACLs, page 13](#)

Enabling or Disabling Additional Validation

You can enable or disable additional validation of ARP packets. By default, no additional validation of ARP packets is enabled.

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.

Procedure

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
 - Step 2** (Optional) From the Summary pane, double-click the device that you want to configure with error-disabled recovery. The Details tab appears in the Summary pane.
 - Step 3** From the Details tab, expand the **Global Settings** section, if necessary.
 - Step 4** (Optional) To enable or disable source MAC address validation, check or uncheck **Source MAC Validation**.
 - Step 5** (Optional) To enable or disable destination MAC address validation, check or uncheck **Destination MAC Validation**.
 - Step 6** (Optional) To enable or disable source and target IP address validation, check or uncheck **IP Address Validation**.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the DAI Logging Buffer Size

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

Procedure

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
 - Step 2** From the Summary pane, click the device whose DAI logging buffer size you want to configure. The Details tab appears in the Summary pane.
 - Step 3** From the Details tab, expand the **Global Settings** section, if necessary. The Total Buffer Size field appears in the Global Settings section.
 - Step 4** Click the **Total Buffer Size** field and enter the maximum number of DAI messages that the buffer can have.
 - Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the DAI System Logging Rate

You can configure the DAI system logging rate. The default DAI system logging rate is five messages every second.



Note The DAI system logging rate is not configurable in Cisco NX-OS Releases 4.0, 4.1, 4.2, and 5.0.

Procedure

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, click the device whose DAI logging buffer size you want to configure. The Details tab appears in the Summary pane.
- Step 3** (Optional) From the Details tab, expand the **Global Settings** section, if necessary. The Log Messages field and the Log Interval (sec) field appear in the Global Settings section. The device sends messages at the rate of the number of messages in the Log Messages field per the number of seconds in the Log Interval (sec) field.
- Step 4** (Optional) Click the **Log Messages** field and enter the number of messages.
- Step 5** (Optional) Click the **Log Interval(sec)** field and enter the number of seconds.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring 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** From the Feature Selector pane, choose **Switching > Layer 2 Security > ARP Inspection**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that has the VLAN that you want to configure with DAI log filtering. The VLANs on the device appear in the Summary pane.
- Step 3** From the Summary pane, click the VLAN that you want to configure with DAI log filtering. The DAI VLAN Details tab appears in the Details pane. On the DAI VLAN Details tab, the DHCP Logging drop-down list appears.
- Step 4** From the DHCP drop-down list, choose the DHCP-binding logging option that you want.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.

Monitoring and Clearing DAI Statistics

A Statistics tab appears in the Details pane when you click a device or VLAN in the Summary pane. When a VLAN is selected, the Statistics tab displays information about DAI that is specific to that VLAN. When a device is selected, the Statistics tab displays information about DAI on all VLANs that are configured to perform DAI.

The following information appears in the Statistics tab:

- DAI Statistics displays information about ARP packets processed.

See the , for more information on collecting statistics for this feature.

Field Descriptions for DAI

Device: Details: Global Settings Section

Table 1: Device: Details: Global Settings Section

Field	Description
Source MAC Validation	Whether the device drops ARP packets when the source MAC address in the Ethernet header does not match the sender MAC address in the ARP message. This field applies to ARP requests and responses. By default, this check box is unchecked.
Destination MAC Validation	Whether the device drops ARP packets when the destination MAC address in the Ethernet header does not match the target MAC address in the ARP message. This field applies to ARP responses only. By default, this check box is unchecked.
IP Address Validation	Whether the device drops ARP packets that contain an invalid IP address for either the sender or target. This field applies to ARP requests and responses. By default, this check box is unchecked.
Total Buffer Size	Number of messages that the DAI log buffer can contain. By default, the buffer size is 64 messages.
Log Messages	Number of DAI log messages for the DAI logging rate limit. The device derives the limit by dividing the value in this field with the value in the Log Interval (sec) field. By default, the number of log messages in the rate limit is five.

Field	Description
Log Interval(sec)	Number of seconds for the DAI logging rate limit. The device derives the limit by dividing the value in the Log Messages field with the value in this field. By default, the number of seconds in the rate limit is 1.

Device: Details: ARP Trust State Section

Table 2: Device: Details: ARP Trust State Section

Figure	Description
Interface	<i>Display only.</i> Name of the Layer 2 interface or the name of the slot containing Layer 2 interfaces.
Trust State	Whether the interface is trusted. When this check box is checked, the device does not trust ARP sources on the interface. By default, this check box is unchecked.

VLAN: DAI VLAN Details Tab

Table 3: VLAN: DAI VLAN Details Tab

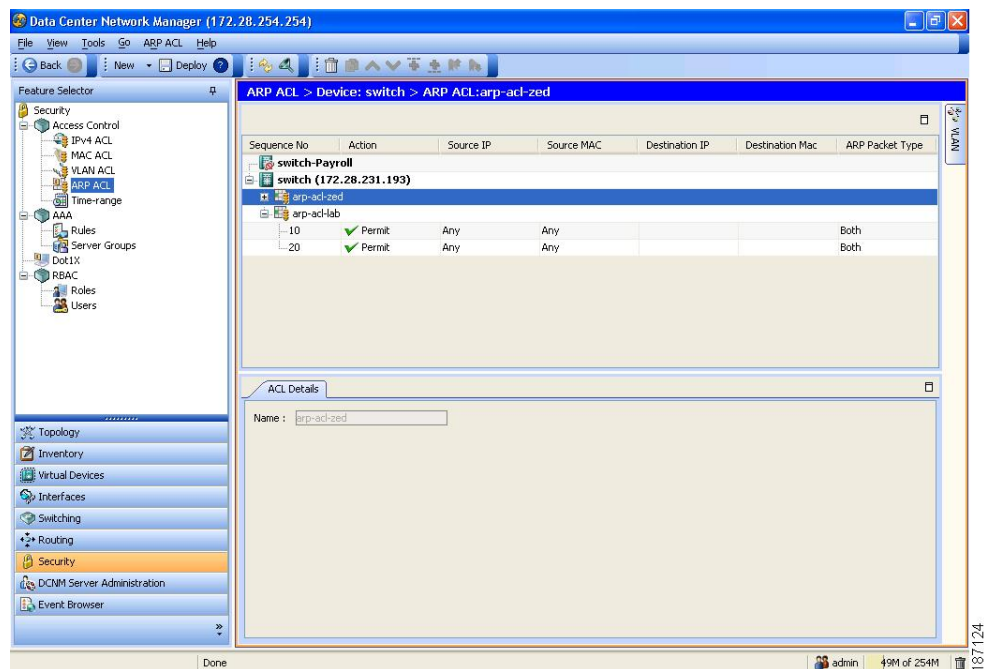
Figure	Description
VLAN	<i>Display only.</i> ID number of the VLAN.
VLAN Name	<i>Display only.</i> Name assigned to the VLAN. By default, VLAN 1 is named Default and all other VLANs are named by combining the text "VLAN" and the four-digit VLAN ID. For example, the default VLAN name for VLAN 50 is VLAN0050.
ARP Inspection	Whether ARP inspection is enabled for the VLAN. When this check box is checked, the device inspects ARP packets received on the VLAN. By default, this check box is unchecked.
ARP Operational State	<i>Display only.</i> Whether ARP inspection is active on the interface.
ARP ACL	Name of the ARP ACL applied to the VLAN. By default, this list is blank.
DHCP Logging	Type of DHCP-binding logging for DAI packets on the VLAN. Valid options are as follows: <ul style="list-style-type: none"> • Permit—DAI packets permitted by DHCP bindings are logged.

Figure	Description
	<ul style="list-style-type: none"> • All—All DAI packets are logged. • Deny—(Default) DAI packets denied by DHCP bindings are logged. • None—No DAI packets are logged.

Configuring ARP ACLs

This figure shows the ARP ACL content pane.

Figure 3: ARP ACL Content Pane



Creating an ARP ACL

You can create an ARP ACL on the device and add rules to it.

Procedure

- Step 1** From the Feature Selector pane, choose **Security** ► **Access Control** ► **ARP ACL**.

Available devices appear in the Summary pane.

- Step 2** From the Summary pane, double-click the device to which you want to add an ACL.
 - Step 3** From the menu bar, choose **File > New > ACL**.
A blank row appears in the Summary pane. The Details tab appears in the Details pane.
 - Step 4** On the Details tab, in the Name field, type a name for the ACL.
 - Step 5** For each rule or remark that you want to add to the ACL, from the menu bar, choose **File > New** and choose **Access Rule** or **Remark**. On the Details tab, configure fields as needed.
 - Step 6** (Optional) If you want to log packets that match a rule in the ACL, check **Log**.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Changing an ARP ACL

You can change, reorder, add, and remove rules in an existing ARP ACL.

Procedure

- Step 1** From the Feature Selector pane, choose **Security > Access Control > ARP ACL**.
Available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that has the ACL that you want to change and then double-click the ACL.
The ACLs on the device and the rules of the ACL that you double-clicked appear in the Summary pane.
- Step 3** (Optional) If you want to change the details of a rule, click the rule in the Summary pane. On the Details tab, configure fields as needed.
- Step 4** (Optional) If you want to add a rule or remark, click the ACL in the Summary pane and then from the menu bar, choose **File > New** and choose **Access Rule** or **Remark**. On the Details tab, configure fields as needed.
- Step 5** (Optional) If you want to remove a rule, click the rule and then from the menu bar, choose **Actions > Delete**.
- Step 6** (Optional) If you want to move a rule or remark to a different position in the ACL, click the rule or remark and then from the menu bar, choose one of the following, as applicable:

- **Actions > Move Up**
- **Actions > Move Down**

The rule moves up or down, as you chose. The sequence number of the rules adjust accordingly.

- Step 7** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Related Topics

- [Creating an ARP ACL](#), page 13

Removing an ARP ACL

You can remove an ARP ACL from the device.

Before You Begin

Ensure that you know whether the ACL is applied to a VLAN. The device allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of VLANs where you have applied the ACL. Instead, the device considers the removed ACL to be empty.

Procedure

-
- Step 1** From the Feature Selector pane, choose **Security** ► **Access Control** ► **ARP ACL**. Available devices appear in the Summary pane.
 - Step 2** From the Summary pane, double-click the device from which you want to remove an ACL. The ACLs currently on the device appear in the Summary pane.
 - Step 3** Click the ACL that you want to remove.
 - Step 4** From the menu bar, choose **Actions** ► **Delete**. A confirmation dialog box appears.
 - Step 5** Choose **Yes**.
DCNM removes the ARP ACL from the device and the ACL disappears from the Summary pane.
You do not need to save your changes.
-

Field Descriptions for ARP ACLs

ARP ACL: ACL Details Tab

Table 4: ARP ACL: ACL Details Tab

Field	Description
Name	Name of the ARP ACL. Names can be a maximum of 64 alphanumeric characters but must begin with an alphabetic character. No name is assigned by default.

ARP Access Rule: ACE Details Tab

Table 5: ARP Access Rule: ACE Details Tab

Field	Description
Sequence Number	Sequence number of the rule. Must be a whole number between 1 and 4294967295. If you add a rule after another rule, the default sequence number is 10 greater than the preceding rule. If you add a rule before another rule, the number is 10 less than the following rule.
Action	Action taken by the device when it determines that the rule applies to the packet. Valid values are as follows: <ul style="list-style-type: none"> • Deny—Stops processing the packet and drops it. • Permit—Continues processing the packet. This is the default value.
Log	Whether the device logs statistics about traffic to which the access rule applies. This check box is unchecked by default.

ARP Access Rule: ACE Details: Source and Destination Section

Table 6: ARP Access Rule: ACE Details: Source and Destination Section

Field	Description
ARP Packet Type	Type of ARP packet that the rule matches: <ul style="list-style-type: none"> • Response—The rule matches ARP responses only. • Both—(Default) The rule matches ARP response and request packets. • Request—The rule matches ARP requests only.
Sender	
IP Type	IP address of the sender, or if Both is selected in the ARP Packet Type list, sender and target. You can choose one of the following radio buttons:

Field	Description
	<ul style="list-style-type: none"> • Any—The rule matches the selected ARP packet type from any IPv4 source. This is the default value. • Host—The rule matches the selected ARP packet type from a specific IPv4 address. When you select this radio button, the IP Address field appears. • Network—The rule matches the selected ARP packet type from an IPv4 network. When you select this radio button, the IP Address field and the Wildcard Mask field appear.
IP Address	IPv4 address of a host or a network. Valid addresses are in dotted decimal format. This field is available when you choose the Host radio button or the Network radio button. This field is unavailable by default.
Wildcard Mask (IP Type)	Wildcard mask of an IPv4 network. Valid masks are in dotted decimal format. For example, if you specified 192.168.0.0 in the IP Address field, you would enter 0.0.255.255 in this field. This field is available when you choose the Network radio button. This field is unavailable by default.
MAC Type	<p>MAC address of sender, or if Both is selected in the ARP Packet Type list, sender and target. You can choose one of the following radio buttons:</p> <ul style="list-style-type: none"> • Any—The rule matches the selected ARP packet type from any MAC source. This is the default value. • Host—The rule matches the selected ARP packet type from a specific MAC address. When you select this radio button, the MAC Address field appears. • Network—The rule matches the selected ARP packet type from a MAC network. When you select this radio button, the MAC Address field and the Wildcard Mask field appear.
MAC Address	MAC address of a host or a network. Valid addresses are in dotted hexadecimal format. This field is available when you choose the Host radio button or the Network radio button. This field is unavailable by default.
Wildcard Mask (MAC Type)	Wildcard mask of a MAC network. Valid masks are in dotted hexadecimal format. For example, if you specified 00c0.4f03.0000 in the MAC Address field, you would enter 0000.0000.ffff in this field. This field is available when you choose the Network radio button. This field is unavailable by default.
Target	

Field	Description
IP Type	<p>IP address of the target. You can choose one of the following radio buttons:</p> <ul style="list-style-type: none"> • Any—The rule matches ARP response packets for any IPv4 target address. This is the default value. • Host—The rule matches ARP response packets for a specific IPv4 target address. When you select this radio button, the IP Address field appears. • Network—The rule matches ARP response packets for an IPv4 network. When you select this radio button, the IP Address field and the Wildcard Mask field appear.
IP Address	IPv4 address of a target host or a network. Valid addresses are in dotted decimal format. This field is available when you choose the Host radio button or the Network radio button. This field is unavailable by default.
Wildcard Mask (IP Type)	Wildcard mask of an IPv4 target network. Valid masks are in dotted decimal format. For example, if you specified 192.168.0.0 in the IP Address field, you would enter 0.0.255.255 in this field. This field is available when you choose the Network radio button. This field is unavailable by default.
MAC Type	<p>MAC address of the target. You can choose one of the following radio buttons:</p> <ul style="list-style-type: none"> • Any—The rule matches ARP response packets for any MAC target address. This is the default value. • Host—The rule matches ARP response packets for a specific target MAC address. When you select this radio button, the MAC Address field appears. • Network—The rule matches ARP response packets for a specific target MAC network. When you select this radio button, the MAC Address field and the Wildcard Mask field appear.
MAC Address	MAC address of a target host or a network. Valid addresses are in dotted hexadecimal format. This field is available when you choose the Host radio button or the Network radio button. This field is unavailable by default.
Wildcard Mask (MAC Type)	Wildcard mask of a target MAC network. Valid masks are in dotted hexadecimal format. For example, if you specified 00c0.4f03.0000 in the MAC Address field, you would enter 0000.0000.ffff in this field. This field is available when you choose the Network radio button. This field is unavailable by default.

ARP ACL Remark: Remark Details Tab

Table 7: ARP ACL Remark: Remark Details Tab

Field	Description
Sequence Number	Sequence number of the remark. The number must be a whole number between 1 and 4294967295. If you add a rule after another rule, the default sequence number is 10 greater than the preceding rule. If you add a rule before another rule, the number is 10 less than the following rule.
Description	Remark text, up to 100 alphanumeric characters. By default, this field is empty.

Additional References for DAI

Standards

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

Feature History for DAI

This table lists the release history for this feature.

Table 8: Feature History for DAI

Feature Name	Releases	Feature Information
Dynamic ARP Inspection	5.2(1)	No change from Release 5.1.
Dynamic ARP Inspection	5.1(1)	No change from Release 5.0.
Dynamic ARP Inspection	5.0(2)	No change from Release 4.2.
Dynamic ARP Inspection	4.2(1)	No change from Release 4.1.

