## Enabling Dynamic ARP Inspection (CLI Procedure)

Dynamic ARP inspection (DAI) protects EX-series switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

To enable dynamic ARP inspection (DAI) on a VLAN or all VLANs using the CLI:

- On a single VLAN (here, the VLAN is employee-vlan):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan arp-inspection
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all arp-inspection
```

**Related Topics**

- Enabling Dynamic ARP Inspection (J-Web Procedure)
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX-series Switch with Access to a DHCP Server Through a Second Switch
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
- Verifying That DAI Is Working Correctly
- Monitoring Port Security
- Understanding DAI for Port Security on EX-series Switches