CCNA Exam Prep: Back to Networking Basics with Hank Preston and Patrick Gargano -- Season 3

Securing the Switch with Essential Layer 2 Protections

Layer 2 device hardening is essential to ensure that your network infrastructure is protected against unauthorized access, MAC spoofing, ARP poisoning, and potential attacks like CAM table overflow or DHCP starvation. Port security limits and identifies MAC addresses on switch ports. DHCP snooping prevents unauthorized DHCP servers from assigning IP addresses, protecting against rogue DHCP attacks. Dynamic ARP inspection (DAI) validates ARP packets to prevent man-in-the-middle attacks by ensuring IP-to-MAC address bindings are correct. Together, these three tools help protect Layer 2 devices from common threats, thereby enhancing the overall security posture of your network infrastructure.

Related CCNA v1.1 exam topic:

- 5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

In this lab, you will explore how to:

- Configure and explore the different Cisco port security options
- Configure and verify DHCP snooping
- Configure and verify DAI

Setup and Scenario

In this set of lab-based demonstrations, you are a network engineer tasked with deploying Layer 2 security on Cisco switches.

You've been asked to:

- Configure port-security
- Configure DHCP snooping
- Configure DAI

*Be sure to **START** the lab **except for the Rogue DHCP** server before continuing*

> Note: The credentials for all devices are **cisco / cisco**
>
> Note: The IOL-L2 image does not support DHCP Snooping or DAI. This lab use the IOSvL2 image instead to demonstrate these features.

Part 1: Reviewing the current network configuration

Before we jump into configuring any Layer 2 security features, let's explore the current network configuration.

Step 1

Open a console connection to the `DSW` switch and use the `show run` command. Some output has been omitted for simplicity.

```
DSW# show run
!
hostname DSW
!
vlan 10
 name CCNAPREP
!
interface GigabitEthernet0/0
 switchport mode access
 switchport access vlan 10
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

Notice that the DSW switch is configured for VLAN 10. DHCP requests from the PCs are forwarded to the Internet (external connector) where the CML server is responding with addresses from the 192.168.255.0/24 network.

Open a console connection to the `ASW` switch and use the `show run` command. Some output has been omitted for simplicity.

```
ASW# show run
!
hostname ASW
!
vlan 10
 name CCNAPREP
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet0/2
 switchport access vlan 10
 switchport mode access
```

```
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet0/3
 switchport access vlan 10
 switchport mode access
 negotiation auto
 spanning-tree portfast edge
!
```

Notice that the ASW switch is configured to support VLAN 10 on interfaces connected to the PCs in the topology. Portfast is enabled to speed up the transition to the STP Forwarding state, ensuring DHCP requests are quickly received and sent to the external CML DHCP server.

The G1/0 interface will be used in Part 5 to connect the DHCP rogue server. The DHCP rogue server will also be turned on in Part 5.

Step 2

Verify the IP address assignment on PC1, PC2, and PC3.

```
PC1:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:11:11:11
          inet addr:192.168.255.227  Bcast:192.168.255.255  Mask:255.255.255.0

PC2:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:22:22:22
          inet addr:192.168.255.175  Bcast:192.168.255.255  Mask:255.255.255.0

PC3:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:33:33:33
          inet addr:192.168.255.123  Bcast:192.168.255.255  Mask:255.255.255.0
```

All three PCs should have received an IP address from the CML DHCP server. Your results might differ from the output above.

Step 3

Verify the MAC table on ASW.

```
ASW# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    5254.0040.4cad    DYNAMIC     Gi0/0
  10    5254.0011.1111    DYNAMIC     Gi0/1
  10    5254.0022.2222    DYNAMIC     Gi0/2
  10    5254.0033.3333    DYNAMIC     Gi0/3
  10    5254.0040.4cad    DYNAMIC     Gi0/0
  10    5254.0054.1adc    DYNAMIC     Gi0/0
Total Mac Addresses for this criterion: 6
```

You should see all three PC's MAC addresses in the MAC table connected to Gi0/1, Gi0/2, and Gi0/3.

PC1 = 5254.0011.1111

PC2 = 5254.0022.2222

PC3 = 5254.0033.3333

These three dynamic MAC addresses will be converted to secure MAC addresses once port security is enabled in the next part of the lab.

Part 2: Configure and explore port security

Let's start by reviewing some of the basics concepts relating to port security.

Recall that there are three ways that a Cisco switch can learn secure MAC addresses:

- **Static** secure MAC addresses that are manually configured on a port.
- **Dynamic** secure MAC addresses that are learned automatically up to a maximum number.
- **Sticky** secure MAC addresses that are dynamically learned and then stored in the running configuration.

There are three types of port security violations:

- **Protect** (quietly drops the offending frame)
- **Restrict** (drops the offending frame, generates a Syslog message and a SNMP trap, and increments the violation counter)
- **Shutdown** (drops the offending frame, the interface is placed in an err-disabled/inactive state, a Syslog message and SNMP trap are generated, and the violation counter is incremented)

Note that there are a few extra optional parameters that can be configured for port security:

- The default maximum number of secure MAC addresses on an interface is **1**.
- The default aging time for dynamic secure MAC addresses is set to **0** and the default aging type is set to **absolute**.
- **Static** secure MAC addresses and **sticky** secure MAC addresses do not age out. The aging time only applies to dynamic secure MAC addresses.

Step 1

Configure a static secure MAC address on port ASW Gi0/1 for PC1. Change the violation type to protect.

```
ASW# config t
ASW(config)# interface gi0/1
```

```
ASW(config-if)# switchport port-security mac-address 5254.0011.1111
ASW(config-if)# switchport port-security violation protect
ASW(config-if)# switchport port-security
ASW(config-if)# exit
```

Step 2

Configure a dynamic secure MAC address on port ASW Gi0/2 for PC2. Change the violation type to restrict. Set the aging time to 30 minutes and the aging type to inactivity.

```
ASW(config)# interface gi0/2
ASW(config-if)# switchport port-security violation restrict
ASW(config-if)# switchport port-security aging time 30
ASW(config-if)# switchport port-security aging type inactivity
ASW(config-if)# switchport port-security
ASW(config-if)# exit
```

Step 3

Configure a sticky secure MAC address on port ASW Gi0/3 for PC3. Keep the default violation of shutdown enabled.

```
ASW(config)# interface gi0/3
ASW(config-if)# switchport port-security mac-address sticky
ASW(config-if)# switchport port-security
ASW(config-if)# exit
ASW(config)# exit
```

Step 4

Verify the port security configuration. To ensure that the dynamic and sticky MAC addresses are learned by the switch, **ping 8.8.8.8 from each PC** before proceeding with the following verification steps.

```
ASW# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Gi0/1              1            1                  0          Protect
      Gi0/2              1            1                  0         Restrict
      Gi0/3              1            1                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

The output above confirms that each port is configured for a default maximum of 1 secure MAC address and that the current count is 1. No violations have occurred yet so the counter shows 0. The last column confirms the current violation mode.

```
ASW# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    5254.0011.1111    SecureConfigured              Gi0/1        -
  10    5254.0022.2222    SecureDynamic                 Gi0/2       26 (I)
  10    5254.0033.3333    SecureSticky                  Gi0/3        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

The output above displays the current secure MAC addresses and how they were learned by the switch, either statically, dynamically, or by using the sticky option. The aging time for PC2 should have started to decrement from configured value of 30 minutes and if no activity is detected before the timer elapses, the dynamic secure MAC address will age out.

```
ASW# show port-security interface Gi0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 5254.0011.1111:10
Security Violation Count   : 0
```

The output above shows the current state of the port security configuration on port Gi0/1. The port is up and the current static secure MAC address will never age out.

```
ASW#show port-security interface gi0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 30 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 5254.0022.2222:10
Security Violation Count   : 0
```

The output above shows the current state of the port security configuration on port Gi0/2. The port is up and the current dynamic secure MAC address will age out after 30 minutes of inactivity.

```
ASW#show port-security interface gi0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 5254.0033.3333:10
Security Violation Count   : 0
```

The output above shows the current state of the port security configuration on port Gi0/3. The port is up and the current sticky secure MAC address will never age out.

Step 5

Change the MAC address on PC1 to cause a port security violation on ASW Gi0/1 and observe the results.

Stop and wipe PC1. Select the Interfaces tab and change the last two hex digits of the MAC address to 00 so that the new MAC address is 5254:0011:1100. Select the checkmark to apply the change and restart the PC. Wait a few moments for PC1 to reboot.

Because interface Gi0/1 is set to a violation mode of protect, you will not see any syslog messages at the AWS switch console and the violation counter will not increment. To confirm that port security is operation, you can see that PC1 did not receive a new IP address from the CML DHCP server and the offending MAC address is shown in the `show port-security interface` output.

Stop and wipe PC1 and reconfigure its original MAC address of 5254:0011:1111.

Step 6

Change the MAC address on PC2 to cause a port security violation on ASW Gi0/2 and observe the results.

Stop and wipe PC2. Select the Interfaces tab and change the last two hex digits of the MAC address to 00 so that the new MAC address is 5254:0022:2200. Select the checkmark to apply the change and restart the PC. Wait a few moments for PC2 to reboot.

Because interface Gi0/2 is set to a violation mode of restrict, you will see multiple syslog messages, as follows:

```
*Oct 17 18:59:46.342: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 5254.0022.2200 on port GigabitEthernet0/2.
```

The message confirms the violating MAC address of 5254:0022:2200 on Gi0/2 but the port remains active. PC2 continue to send DHCP Discover messages to ASW causing an increasing number of violations. You can see the violation counter increase by using the `show port-security` command.

Stop and wipe PC2 and reconfigure its original MAC address of 5254:0022:2222.

Step 7

Change the MAC address on PC3 to cause a port security violation on ASW Gi0/3 and observe the results.

Stop and wipe PC3. Select the Interfaces tab and change the last two hex digits of the MAC address to 00 so that the new MAC address is 5254:0033:3300. Select the checkmark to apply the change and restart the PC. Wait a few moments for PC3 to reboot.

Because interface Gi0/3 is set to a violation mode of shutdown, you will see multiple syslog messages, as follows:

```
ASW#
*Oct 17 19:09:42.050: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/3, putting Gi0/3 in err-disable state
ASW#
*Oct 17 19:09:42.050: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 5254.0033.3300 on port GigabitEthernet0/3.
ASW#
*Oct 17 19:09:43.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to down
ASW#
*Oct 17 19:09:44.050: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to down
```

The message confirms the violating MAC address of 5254:0033:3300 on Gi0/3 and the port is put into the `err-disable` state and the interface is placed in the down/down state. Use the following commands to investigate the port security violation:

```
ASW# show interfaces status err-disabled
Port         Name         Status       Reason              Err-disabled Vlans

Gi0/3                     err-disabled psecure-violation

ASW# show port-security int gi0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 5254.0033.3300:10
Security Violation Count   : 1
```

PC3 will continue to send DHCP Discover messages but these are dropped by ASW since the Gi0/3 interface is in a `Secure-shutdown` state. The offending MAC address is shown in the output and the violation counter was incremented to 1.

Stop and wipe PC3 and reconfigure its original MAC address of 5254:0033:3333.

Doing so will not automatically bring the Gi0/3 interface out of its `err-disabled` state. There are two ways of reenabling Gi0/3:

Option 1: Manually reenable the port by entering `shutdown` followed by `no shutdown` on Gi0/3 once the offending MAC has been removed.

Option 2: Enter the `errdisable recovery cause psecure-violation` global configuration command on ASW. The default timeout for recovery is 5 minutes. You can adjust the recovery time with the following command:

```
errdisable recovery intervale time-interval
```

The following output shows what is displayed at the console when using the automatic recovery feature on a Cisco switch:

```
ASW#
*Oct 17 19:30:04.306: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Gi0/3
ASW#
*Oct 17 19:30:06.306: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
ASW#
*Oct 17 19:30:07.306: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to up
ASW#
```

Ensure that Gi0/3 is up/up before continuing the lab.

Stop and restart PC1, PC2 and PC3, and verify that they can ping 8.8.8.8 before continuing to Part 3 of the lab.

Part 3: Configure and verify DHCP Snooping

In Part 3 you will enable DHCP snooping on ASW for VLAN 10 and ensure that the trunk link to DSW is trusted since that is the uplink that will received legitimate DHCP messages from the CML DHCP server. You will also configure DHCP snooping on DSW.

Step 1

On ASW, globally enable DHCP snooping and enable it for VLAN 10. Configure DHCP snooping MAC address validation and limit the number of DHCP messages to 10 packets per second on all untrusted ports. Configure Gi0/0 as a DHCP snooping trusted port.

```
ASW(config)# ip dhcp snooping
ASW(config)# ip dhcp snooping vlan 10
ASW(config)# ip dhcp snooping verify mac-address
ASW(config)# interface range gi0/1-3
ASW(config-if-range)# ip dhcp snooping limit rate 10
ASW(config-if-range)# interface gi0/0
ASW(config-if)# ip dhcp snooping trust
```

Step2

Verify the DHCP snooping configuration.

```
ASW# show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
 Proxy bridge is configured on following VLANs:
none
 Proxy bridge is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0e00 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
GigabitEthernet0/0       yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet0/1       no         no              10
  Custom circuit-ids:
GigabitEthernet0/2       no         no              10
  Custom circuit-ids:
GigabitEthernet0/3       no         no              10
  Custom circuit-ids:
```

Verify the MAC to IP snooping bindings that are built by ASW:

```
ASW# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
52:54:00:33:33:33   192.168.255.123  3577        dhcp-snooping   10    GigabitEthernet0/3
52:54:00:11:11:11   192.168.255.227  3563        dhcp-snooping   10    GigabitEthernet0/1
52:54:00:22:22:22   192.168.255.175  3570        dhcp-snooping   10    GigabitEthernet0/2
Total number of bindings: 3
```

> Note: If the DHCP snooping binding table is empty, you can use the `sudo service networking restart` command to force all three PCs to trigger a fresh DHCP request, or use the `sudo udhcpc -R -i eth0` command.

Step 3

On DSW, globally enable DHCP snooping and enable it for VLAN 10. Configure Gi0/1 as a DHCP snooping trusted port.

```
DSW(config)# ip dhcp snooping
DSW(config)# ip dhcp snooping vlan 10
DSW(config)# int g0/1
DSW(config-if)# ip dhcp snooping trust
```

Step 4

Release and renew the DHCP IP address on PC1. Observe the result.

```
PC1:~$ sudo  udhcpc -R -i eth0
udhcpc: started, v1.37.0
udhcpc: broadcasting discover
udhcpc: broadcasting discover
udhcpc: broadcasting discover
udhcpc: broadcasting discover
^C
PC1:~$
```

Notice the syslog message that is displayed at the DSW console port:

```
*Oct 20 18:07:54.063: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or option82 value on untrusted port, messa
```

Because DHCP snooping is enabled on ASW, it automatically adds Option 82 information to the DHCP messages received from PC1. Option 82 was defined in RFC 3046 and serves to identify both the DHCP relay agent (if any) and the client that sent the DHCP Discover message.

DSW automatically drops the DHCP Discover messages from PC1 with Option 82 since it arrives on a DHCP snooping untrusted port. There are two solutions to remedy this:

- Configure ASW to not insert the Option 82 information when it receives the DHCP Discovery message from PC1, or
- Configure DSW G0/0 to allow Option 82 information on an untrusted port.

Since DSW is not acting as a DHCP relay agent, we will disable the insertion of Option 82 at the source on both ASW and DSW. The reason DSW needs to also be configured in this way is that it is performing DHCP snooping and will reinsert Option 82 as it forwards the DHCP Discovery message to the CML DHCP server.

```
ASW(config)# no ip dhcp snooping information option
DSW(config)# no ip dhcp snooping information option
```

Part 4: Configure and verify Dynamic ARP Inspection

In Part 4 you will enable DAI for VLAN 10 on ASW and ensure that the trunk link to DSW is trusted since that is the uplink that will received legitimate ARP messages. Recall that DHCP snooping is required for DAI.

Step 1

On ASW, enable DAI for VLAN 10. Configure Gi0/0 as a DAI trusted port. Adjust the rate limiting for ARP messages to 10 packets per second. Enable source MAC validation.

```
ASW(config)# ip arp inspection vlan 10
ASW(config)# ip arp inspection validate src-mac
ASW(config)# int gi0/0
ASW(config-if)# ip arp inspection trust
ASW(config)# int range gi0/1-3
ASW(config-if-range)# ip arp inspection limit rate 10
```

Step 2

Verify DAI.

From the console on PC1, ping PC2 to generate some traffic and ARP requests. **The IP address for PC2 in your lab will differ from the example below.**

```
PC1:~$ ping 192.168.255.175
PING 192.168.255.175 (192.168.255.175): 56 data bytes
64 bytes from 192.168.255.175: seq=0 ttl=42 time=8.138 ms
64 bytes from 192.168.255.175: seq=1 ttl=42 time=2.421 ms
PC1:~$ ^C

PC1:~$
```

Use the `show ip arp inspection` command on ASW to confirm that DAI is correctly configured.

```
ASW#sh ip arp inspection

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

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

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

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   10             10              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   10              7              0              0                     0

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

```
 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   10                   0                        0                      0
```

The output confirms that ARP messages are being inspected for VLAN 10 and that no ARP messages have been dropped. The output also tracks DHCP messages that were inspected and permitted.

Part 5: Testing DHCP Snooping

In Part 5, you will connect the rogue DHCP server to interface Gi1/0 on ASW and observe how the switch responds.

Step 1

On ASW, enable DHCP snooping debugging.

```
ASW# debug ip dhcp snooping events
```

Step 2

Start the rogue DHCP server CML node by right-clicking it and selecting **Start**.

Within a few seconds of the rogue DHCP server starting up, the ASW console should display messages indicating DAI and DHCP snooping are intercepting rogue DHCP messages:

```
*Oct 27 14:09:29.151: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/0, vlan 10.([5254.00e5.8f80/192.168.255.1/0000.0000.0000/192.168.255.25/14:09:2
*Oct 27 14:09:30.151: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/0, vlan 10.([5254.00e5.8f80/192.168.255.1/0000.0000.0000/192.168.255.25/14:09:2
*Oct 27 14:09:31.175: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/0, vlan 10.([5254.00e5.8f80/192.168.255.1/0000.0000.0000/192.168.255.25/14:09:3
*Oct 27 14:09:31.405: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message type: DHCPOFFER, MAC sa: 5254.00e5.8
```

Notice that the packets are getting dropped but that the interface remains in the up/up state.

Disable all debugging with the `no debug all` command.

Step 3

Verify DHCP snooping and DAI activity.

```
ASW# show ip dhcp snooping statistics
 Packets Forwarded                                = 100
 Packets Dropped                                  = 41
 Packets Dropped From untrusted ports             = 41

ASW# show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   10             32             17             17              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   10             16              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   10                   0                        0                      0
```

The number of packets dropped will continue to increase as the rogue DHCP server continues to send DHCP Offer messages into the network.

Congratulations! You have completed the lab. You learned how to configure and verify Layer 2 security using port security, DHCP snooping and DAI.