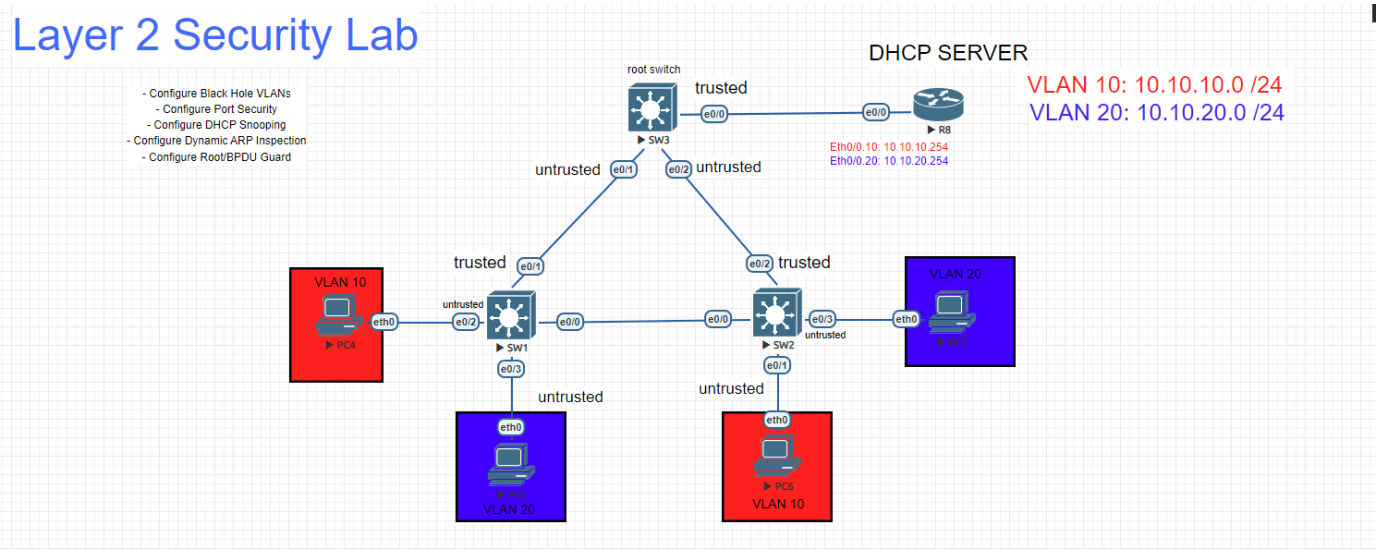
Dynamic ARP Inspection

- The Address Resolution protocol is used to map Layer 3 to Layer 2 addresses in our networks. Endpoints and network devices will have a ARP Cache/Table for those mappings. In our networks someone malicious could spoof ARP replies and perform MITM attacks. this is called "ARP Spoofing", we can authenticate ARP packets by implementing DAI (Dynamic ARP Inspection).

- DAI in a DHCP environment will rely on the DHCP snooping binding database table to authenticate the Layer 3 - Layer 2 mappings in ARP requests and replies.



- For this How to we will first need to get our network ready by configuring VLANs, Trunks and DHCP snooping. If you do not know how to configure these technologies please refer to our other How To's. To configure DAI follow the configuration below.

`SW3(config)#ip arp inspection vlan 10,20` # This command will enable ARP inspection for the specified VLANs. DAI will authenticate the Layer 2 and Layer 3 mappings for devices in your network to prevent spoofing.

```
SW3(config)#ip arp inspection vlan 10,20
SW3(config)#
```

```
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#
*Dec  6 15:42:20.477: %SYS-5-CONFIG_I: Configured from console by console
SW2(config)#ip arp inspection vlan 10,20
SW2(config)#
```

Verification. Now that we have enabled DAI on all our switches lets clear the arp cache in our DHCP server and resend the DHCP request from our clients.

`R1#clear arp` # This command will clear the ARP table in our Cisco iOS router.

```
DHCP#clear arp
DHCP#
```

```
SW3(config)#
*Dec  6 15:43:44.716: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/
0, vlan 10.([aabb.cc00.8000/10.10.10.254/ffff.ffff.ffff/10.10.10.254/15:43:44 UT
C Tue Dec 6 2022])
*Dec  6 15:43:44.717: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Et0/
0, vlan 20.([aabb.cc00.8000/10.10.20.254/ffff.ffff.ffff/10.10.20.254/15:43:44 UT
C Tue Dec 6 2022])
```

Here we can see an error message for our DHCP server. This is because the DHCP server is a static address and is not in our DHCP snooping binding table. We can fix this issue with an "ARP ACL" or by configuring the "ARP Trust" command on interfaces facing the DHCP server.

`SW3(config)#interface eth0/0` # Brings you into the interface subconfiguration mode

`SW3(config-if)#ip arp inspection trust` # This command allows ARP packets to be authenticated without the L2-L3 mappings being in the DHCP snooping table

`SW2(config)#arp access-list DAI` # This command creates an ACL specifically for ARP packets

`SW2(config-arp-acl)#permit ip host 10.10.10.254 host aabb.cc00.8000` # This command permits a specific host on the ARP ACL

`SW2(config-arp-acl)#permit ip host 10.10.20.254 host aabb.cc00.8000` # This command permits a specific host on the ARP ACL

`SW2(config)#ip arp inspection filter DAI vlan 10,20` # This command will apply the the ARP ACL for the specified VLANs.

Full configuration below

```
SW3(config)#int eth0/0
SW3(config-if)#ip arp inspection trust
SW3(config-if)#
```

```
SW2(config)#arp access-list DAI
SW2(config-arp-nacl)#permit ip host 10.10.10.254 mac host aabb.cc00.8000
SW2(config-arp-nacl)#permit ip host 10.10.20.254 mac host aabb.cc00.8000
SW2(config-arp-nacl)#exit
SW2(config)#ip arp inspection filter DAI vlan 10,20
SW2(config)#
```

Show commands

```
SW2#show ip arp inspection

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

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Active      DAI                No
   20     Enabled          Active      DAI                No

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

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   10              0              0              0              0
   20             30              0              0              0

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

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   20             30              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   10                    0                        0                      0
   20                    0                        0                      0
SW2#
```