# DYNAMIC ARP INSPECTION

Dynamic Address Resolution Protocol (Dynamic ARP) inspection is a security feature that validates ARP packets in the network.

Without dynamic ARP inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Dynamic ARP inspection prevents this type of attack. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table.

When you enable Dynamic ARP inspection, ARP packets on untrusted ports are filtered based on the source MAC and IP addresses stored in the DHCP snooping table. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the DHCP snooping table. Otherwise, the ARP packet is dropped.

For dynamic ARP inspection to function, DHCP snooping must be globally enabled. Dynamic ARP inspection is configured on a VLAN to VLAN basis.

Let’s enable Dynamic ARP Inspection on VLANs 10, 11 and set our uplinks as trusted;

```
ip arp-inspection vlan 10

ip arp-inspection vlan 11

ip arp-inspection enable
```

```
interface fa 1/24,2/24

 ip arp-inspection trusted

exit

interface fa 1/1-23,2/1-23

 ip arp-inspection untrusted

exit
```

**Issues with Dynamic ARP Inspection**

Dynamic ARP Inspection relies on the information stored in the DHCP binding table (from DHCP Snooping) to validate the ARP packets it receives on untrusted ports. Any device whether it be statically configured or dynamically configured would need to appear in the DHCP binding table.

If you have a statically configured device you'll need to manually populate the DHCP snooping table. If someone changed out a statically configured device the MAC address would most likely need to be updated in the DHCP binding table. If the DHCP binding table was accidentally cleared the switch would block IP traffic until the DHCP binding table was re-built either manually or from DHCP transactions.

This is another great reason to use manual or reserved DHCP assignments where possible if the device requires a persistent IP address.

This feature will likely create some significant administrative overhead based on the number of devices configured with a static IP address over the number of DHCP configured devices.

Source : http://blog.michaelfmcnamara.com/2013/01/dhcp-snooping-arp-inspection-ip-source-guard/