Dynamic ARP Inspection (DAI)

Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. A malicious user could intercept traffic intended for other hosts on the LAN segment and poison the ARP caches of connected systems by broadcasting forged ARP responses.

Several known ARP-based attacks can have a devastating impact on data privacy, confidentiality, and sensitive information. To block such attacks, the Layer 2 switch must have a mechanism to validate and ensure that only valid ARP requests and responses are forwarded.

DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

DAI ensures that only valid ARP requests and responses are relayed. The switch 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

•It forwards all ARP packets received on a trusted interface without any checks

•DAI determines the validity of an ARP Packet based on the valid MAC address-to-IP address bindings stored in the DHCP snooping database

•DAI is supported on access ports,trunk ports,EtherChannels and private VLAN ports.

•DAI is an ingress security feature,it does not perform any egress checking.

•DAI is not effective for hosts connected to router that do not support DAI or do not have this feature enabled.

This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

Enable arp inspection

Switch(config)# ip arp inspection vlan <vlan-range>