DHCP Snooping

DHCP snooping is a Layer 2 security feature that acts like a firewall between DHCP clients and DHCP servers. The primary purpose is to prevent rogue DHCP servers from offering an IP address to clients. The rogue or unauthorized DHCP server attempts to respond to DHCP requests from clients. It is commonly referred to as a man-in-the-middle attack (MITM).

DHCP snooping enables trusted switch ports that are connected directly to an authorized DHCP server. Any frames that do not originate from an authorized DHCP server are dropped. In addition, there is a system error message logged. The following services are provided by DHCP snooping.

- Permit DHCP packets on DHCP trusted port only.
- Prevent rogue DHCP servers from offering IP address to hosts.

DHCP snooping is enabled both globally per access switch and per VLAN. The network administrator would enable snooping on VLAN/s assigned to switch access ports. It is enabled on any uplink to the router as well. Typically you would enable all host VLANs for DHCP snooping. For DHCP snooping to work properly, all authorized DHCP servers must be connected to the switch through trusted interfaces. All untrusted DHCP messages are forwarded only to trusted interfaces as well.

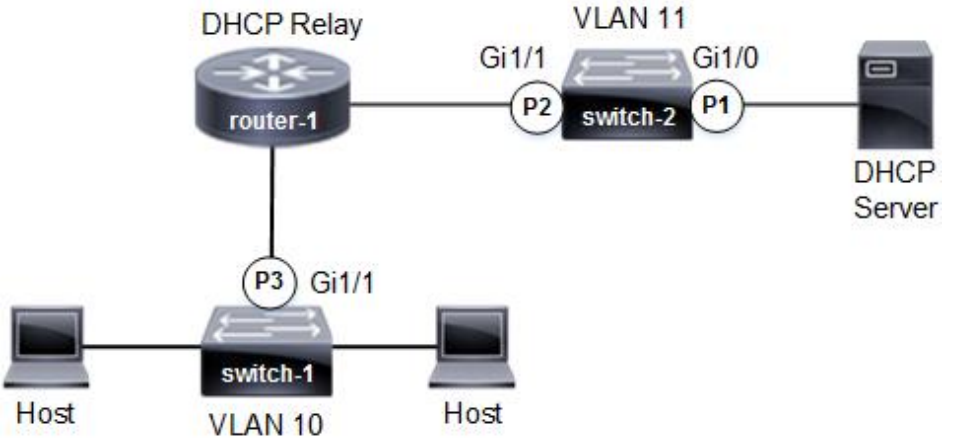
Switch Port Trusted Interface Operation

- DHCP snooping trust interfaces are enabled on a Layer 2 Ethernet switch port or port channel to forward all DHCP broadcast messages.
- Only Layer 2 trusted interfaces forward all DHCP broadcast messages.
- Enable trusted interfaces on switch port connected to DHCP server and uplink to router. That enables trusted connectivity between host and DHCP server.
- All untrusted DHCP messages are forwarded only to trusted interfaces.

Example: DHCP Snooping

Refer to the network topology drawing. Select the network point where DHCP snooping trust interface is enabled?

Figure 1 DHCP Snooping



Answer

DHCP snooping trust interfaces are enabled on switch-2. The trusted interface **P1** connects directly to DHCP server where DHCP messages are sent and received. The switch port **P2** is enabled as a trusted interface for packets to the router. There is a trusted interface configured on switch-1 port **P3** as well. The trusted forwarding path is then enabled for DHCP packets between host and DHCP server.

DHCP Snooping Configuration

The following IOS commands enables DHCP snooping globally on switch-1 and switch-2. Trusted interfaces are enabled for the forwarding path between hosts and DHCP server. The IOS commands are only supported on switch port interfaces.

Switch-1 Configuration

ip dhcp snooping *(enable globally)*
ip dhcp snooping vlan 10 *(enable snooping on vlan 10)*
interface gigabitethernet1/1 *(uplink to router)*
ip dhcp snooping trust *(configure trusted interface)*

Switch-2 Configuration

ip dhcp snooping *(enable globally)*
ip dhcp snooping vlan 11 *(enable snooping on vlan 11)*
interface gigabitethernet1/1 *(uplink to router)*
ip dhcp snooping trust *(configure trusted interface)*
interface gigabitethernet1/0 *(link to DHCP server)*
ip dhcp snooping trust *(configure trusted interface)*

Configure switch ports with DHCP clients (hosts) as untrusted with **no ip dhcp snooping trust** interface level command. Verify DHCP snooping is operational on switch-1 and switch-2.

switch# **show ip dhcp snooping**

Dynamic ARP Inspection (DAI)

Cisco Dynamic ARP Inspection is a Layer 2 security feature configured on access switches. The purpose is to prevent man-in-the-middle (MITM) hacker attacks based on ARP spoofing. For example, a network device plugged into the network could broadcast ARP replies on the local subnet. The device could attempt to spoof as a default gateway for example. ARP replies then appear to originate from the actual default gateway router. The attacks cause ARP table poisoning.

All access switches with host VLANs should have Dynamic ARP Inspection enabled. In fact DHCP snooping must be configured as well to prevent MITM attacks. Cisco switches inspect ARP packet and do lookup in DHCP snooping table to validate entry. ARP reply packets have the MAC address and IP address of sender.

The switch drops any malicious or corrupt ARP packets when sender MAC address and IP address entry does not match in DHCP snooping table. In addition, there is also a system error message logged.

Enable dynamic ARP inspection on VLAN 10 to detect and prevent ARP spoofing. This is a global command that is enabled on switch VLANs.

switch(config)# **ip arp inspection vlan 10**
switch# **show ip arp inpection**