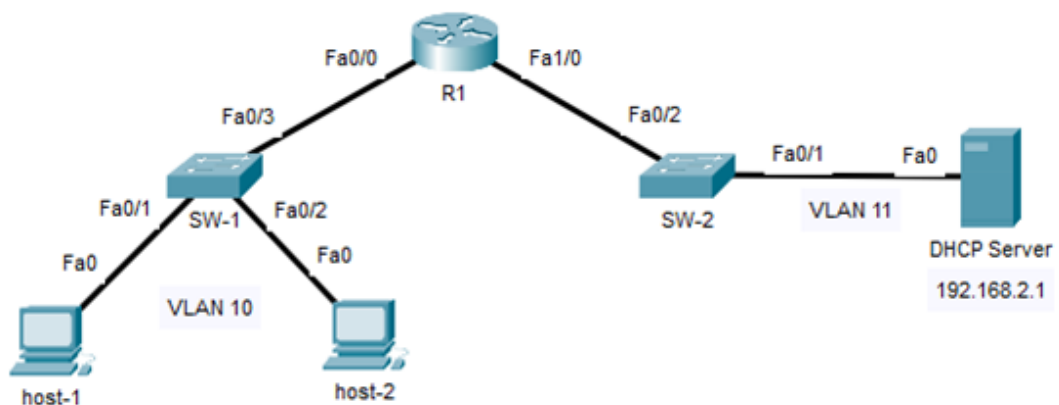


DHCP Snooping

Lab Summary

Enable DHCP snooping to prevent unauthorized (rogue) DHCP servers from sending IP addressing to DHCP hosts.

Figure 1 Lab Topology



Lab Configuration

Start Packet Tracer File: **dhcp snooping.pkt**

Click on *SW-1* icon and select *CLI* folder.

Step 1: Enter global configuration mode

```
SW-1> enable
SW-1# configure terminal
```

Step 2: Enable DHCP Snooping globally on SW-1.

```
SW-1(config)# ip dhcp snooping
```

Step 3: Enable DHCP Snooping for VLAN 1 and VLAN 10.

```
SW-1(config)# ip dhcp snooping vlan 1,10
```

Step 4: Enable SW-1 interface Fa0/3 uplink as trusted with rate limiting of packets.

```
SW-1(config)# interface fastethernet0/3
SW-1(config-if)# ip dhcp snooping trust
SW-1(config-if)# ip dhcp snooping limit rate 40
SW-1(config-if)# exit
```

Click on *SW-2* icon and select *CLI* folder.

Step 5: Enter global configuration mode

```
SW-2> enable  
SW-2# configure terminal
```

Step 6: Enable DHCP Snooping globally on SW-2.

```
SW-2(config)# ip dhcp snooping
```

Step 7: Enable DHCP Snooping for VLAN 1 and VLAN 11.

```
SW-2(config)# ip dhcp snooping vlan 1,11
```

Step 8: Enable SW-2 interface Fa0/1 uplink as trusted with rate limiting of packets.

```
SW-2(config)# interface range fastethernet0/1  
SW-2(config-if)# ip dhcp snooping trust  
SW-2(config-if)# ip dhcp snooping limit rate 40
```

Step 9: Enable SW-2 interface Fa1/1 uplink as trusted with rate limiting of packets.

```
SW-2(config)# interface range fastethernet1/1  
SW-2(config-if)# ip dhcp snooping trust  
SW-2(config-if)# ip dhcp snooping limit rate 40  
SW-2(config-if)# exit
```

Click on *R1* icon and select *CLI* folder.

Step 10: Enter global configuration mode

```
R1> enable  
R1# configure terminal
```

Step 11: Configure DHCP relay on R1 LAN interface Fastethernet0/0.

```
R1(config)# interface fastethernet0/0  
R1(config)# ip helper-address 192.168.2.1  
R1(config-if)# end  
R1# copy running-config startup-config
```

Click on *SW-1* icon and select *CLI* folder.

Step 12: Enable dynamic ARP inspection on VLAN 1 and VLAN 10 to detect ARP table poisoning and prevent man in the middle attacks.

```
SW-1(config)# ip arp inspection vlan 1,10
```

Step 13: Configure interface Fa0/3 as trusted for ARP inspection.

```
SW-1(config)# interface fastethernet 0/3
SW-1(config-if)# ip arp inspection trust
SW-1(config-if)# end
SW-1# copy running-config startup-config
```

Click on SW-2 icon and select *CLI* folder.

Step 14: Enable dynamic ARP inspection for VLAN 1 and VLAN 11 to detect ARP table poisoning and prevent man in the middle attacks.

```
SW-2(config)# ip arp inspection vlan 1,11
```

Step 15: Configure interface Fa0/1 and Fa0/2 as trusted for ARP inspection.

```
SW-2(config)# interface fastethernet 0/1
SW-2(config-if)# ip arp inspection trust
SW-2(config-if)# interface fastethernet 0/2
SW-2(config-if)# ip arp inspection trust
SW-2(config-if)# end
SW-2# copy running-config startup-config
```

Step 16: Verify Lab

Verify DHCP snooping and ARP inspection is operational on SW-1 and SW-2.

```
SW-1# show ip dhcp snooping
SW-2# show ip dhcp snooping
SW-1# show ip arp inspection vlan 10
SW-2# show ip arp inspection vlan 11
```

DHCP Snooping

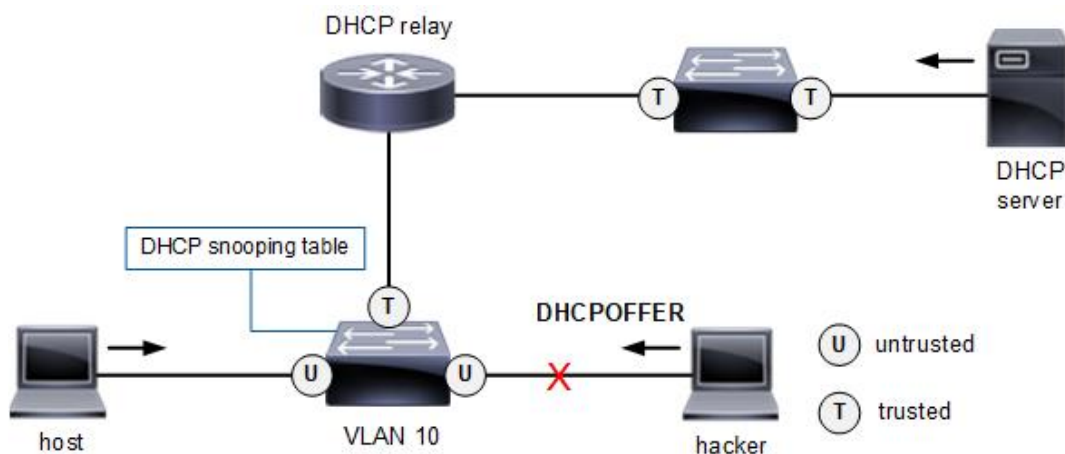
DHCP snooping prevents unauthorized (rogue) hosts from spoofing a legitimate DHCP server with man-in-the-middle (MITM) attack. The hacker machine responds to DHCPDISCOVER and DHCPREQUEST messages from DHCP clients on the local subnet before a legitimate DHCP server does. This is the result of DHCP server being located on a different subnet than clients.

DHCP snooping is a Layer 2 security feature that acts like a firewall between DHCP clients and DHCP servers. The security protocol builds a database table on a switch with IP-to-MAC bindings and VLAN membership.

This is accomplished using information extracted from DHCP messages intercepted between client and DHCP server. DHCP snooping drops DHCPOFFER messages on an untrusted switch port or when source MAC address of host does not match binding table entries. This prevents DHCP server spoofing from a hacker machine connected to a switch.

DHCP snooping is configured per VLAN on Cisco switches. All access edge (host) switch ports are untrusted by default and uplinks to network devices should be explicitly configured with trusted state. Untrusted DHCP messages from hosts are only forwarded to DHCP server via trusted interfaces.

Figure 2 DHCP Snooping



Configure DHCP snooping globally on the switches and also enable on at least one VLAN. This should be done as a last step to prevent disable of DHCP services while doing the configuration.

```
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping vlan 1,10
```

The following interface-level commands enable a trusted interface on the forwarding path to a DHCP server and rate limiting. This would also include the switch port connected to DHCP server. This feature is supported on access, trunk, and EtherChannel physical interfaces.

```
switch(config-if)#ip dhcp snooping trusted  
switch(config-if)#ip dhcp snooping limit rate 100
```

Dynamic ARP Inspection

Dynamic ARP inspection (DAI) is a Layer 2 security feature configured on Cisco switches. The purpose of DAI is to prevent man-in-the-middle (MITM) hacker attacks based on ARP spoofing. ARP protocol operation permits gratuitous ARP (GARP) replies from devices to update any MAC address or IP address changes. This triggers a normal update of ARP tables on all Layer 3 network devices. The hacker machine sends gratuitous ARP reply with an IP address already assigned on the network and local MAC address of machine to poison the ARP cache.

For example, ARP spoofing could replace the ARP table entry on a switch for a default gateway. The hacker machine would send GARP reply with IP address of default gateway and local MAC address. All traffic is then redirected to the hacker machine based on the new spoofed ARP mapping of IP-to-MAC binding. This is referred to as a man-in-the-middle (MITM) attack.

Configure dynamic ARP inspection on all host VLANs where DHCP addressing is enabled. DHCP snooping is also required to build a table with IP-to-MAC bindings and VLAN membership learned from DHCP traffic to hosts. This centralized database on a switch is then used to validate ARP packets. For DHCP snooping to work properly, all authorized DHCP servers must be connected in the forwarding path to hosts through trusted interfaces. All untrusted DHCP messages from hosts are only forwarded only to trusted interfaces.

Cisco access edge ports are all untrusted by default and subject to ARP validation since hacker attack would originate from an access edge port. ARP packets that fail validation are intercepted, dropped, and error message logged to prevent ARP spoofing. The switch drops any ARP packets where the sender MAC address and IP address do not match any entry in the DHCP snooping table. There is also the option to add static IP-to-MAC entries to the ARP table.

All switch ports connecting to other network devices should be explicitly configured as trusted state. There is support for dynamic ARP inspection on access, trunk, and EtherChannel interfaces. Note that dynamic ARP inspection is ingress direction only and can be enabled globally or per interface.

This global command enables dynamic ARP inspection (DAI) for all DHCP hosts assigned to VLAN 10.

```
switch(config)#ip arp inspection vlan 10
```

This interface-level command configures all uplink ports to network devices as trusted state.

```
switch(config-if)#ip arp inspection trust
```

This command will display the operational status of DAI along with configuration settings and dropped packets for VLAN 10. This command also displays per physical interface as well.

```
switch#show ip arp inspection vlan 10
```