# Troubleshoot Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG) in Catalyst Switches

## Contents



## Introduction

This document describes how Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG) work, and how to validate them in Catalyst 9K Switches.

## DHCP Snooping and Related Features

Before diving into DAI and IPSG, you need to discuss briefly about DHCP Snooping, which is a pre-requisite to DAI and IPSG.

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

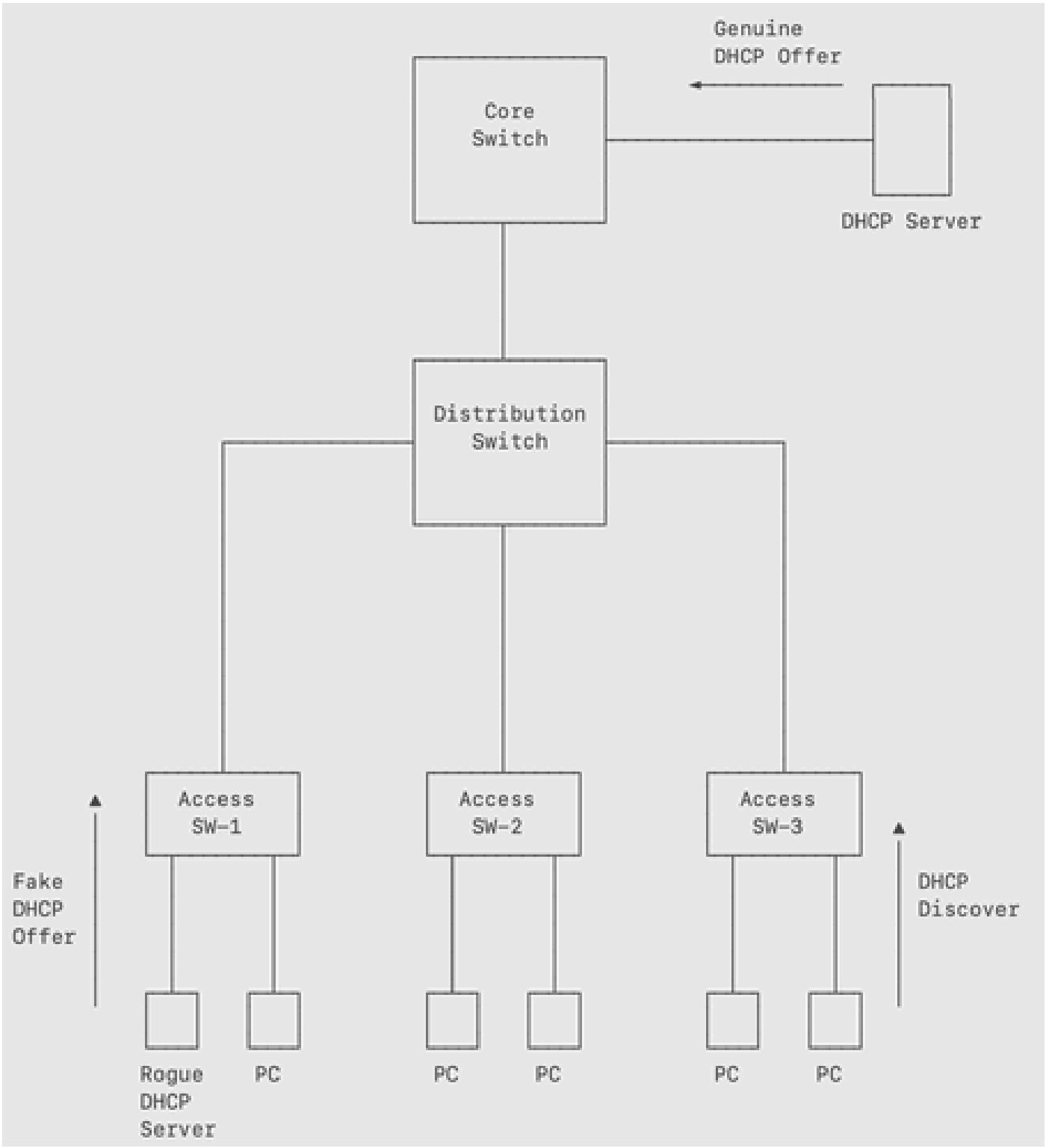
DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs these activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

DAI is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC addresses to IP address bindings. This capability protects the network from certain “man-in-the-middle” attacks.

IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IPSG to prevent traffic attacks if a host tries to use the IP address of its neighbor.

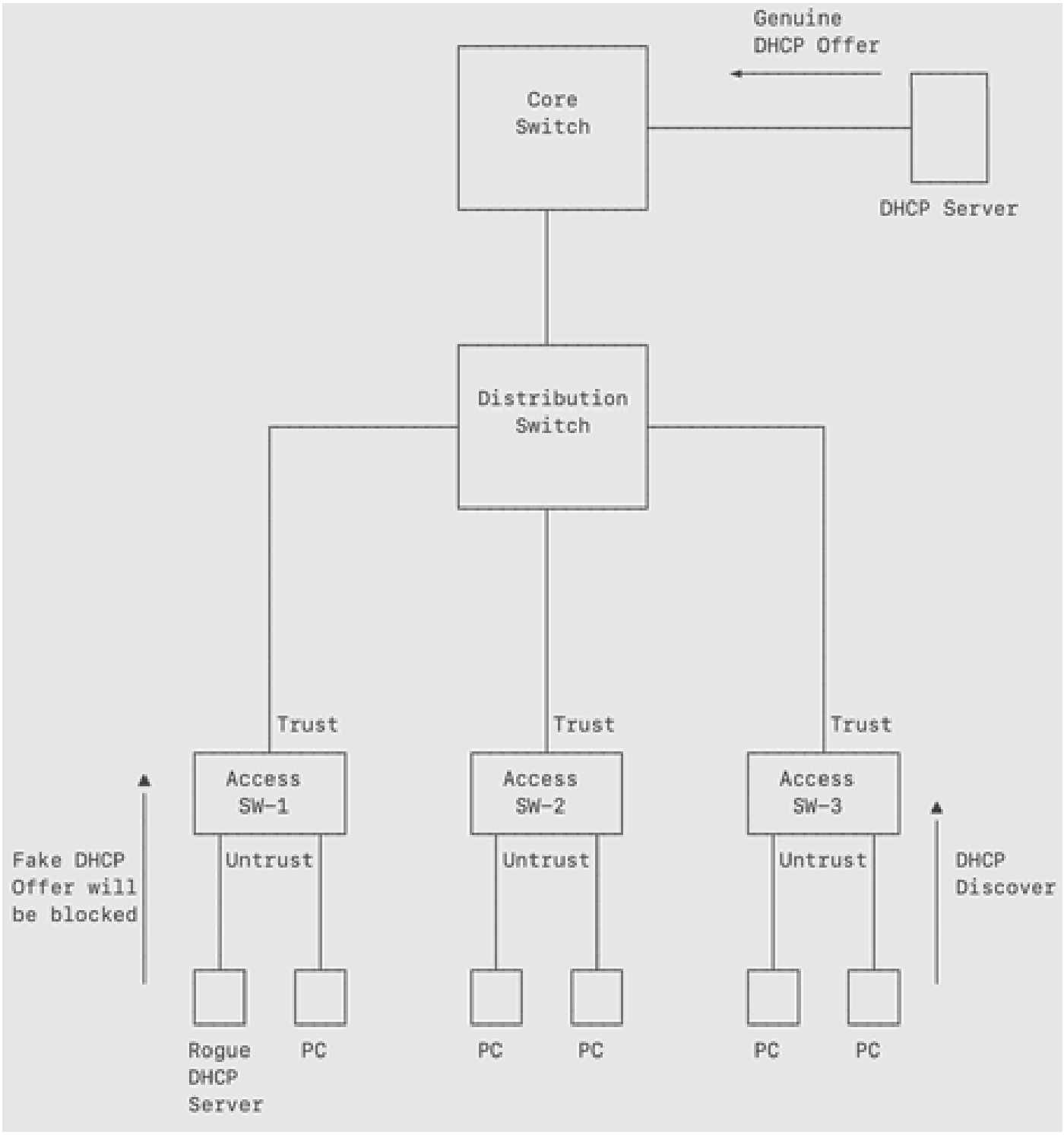
## Scenario without DHCP Snooping




1. In this diagram, you can see that multiple clients would like to receive an IP address from the DHCP server that is connected to the Core Switch.
2. However, there is a malicious/rogue DHCP server that is connected to one of the access layer switches that can receive the DHCP discovers and send out DHCP offers faster than the actual DHCP server.
3. The attacker can set the gateway address in the offer message in such a way that it can receive all the traffic from the client, thus compromising on confidentiality of the communication.

4. This is known as the Man In The Middle attack.

## Scenario with DHCP Snooping

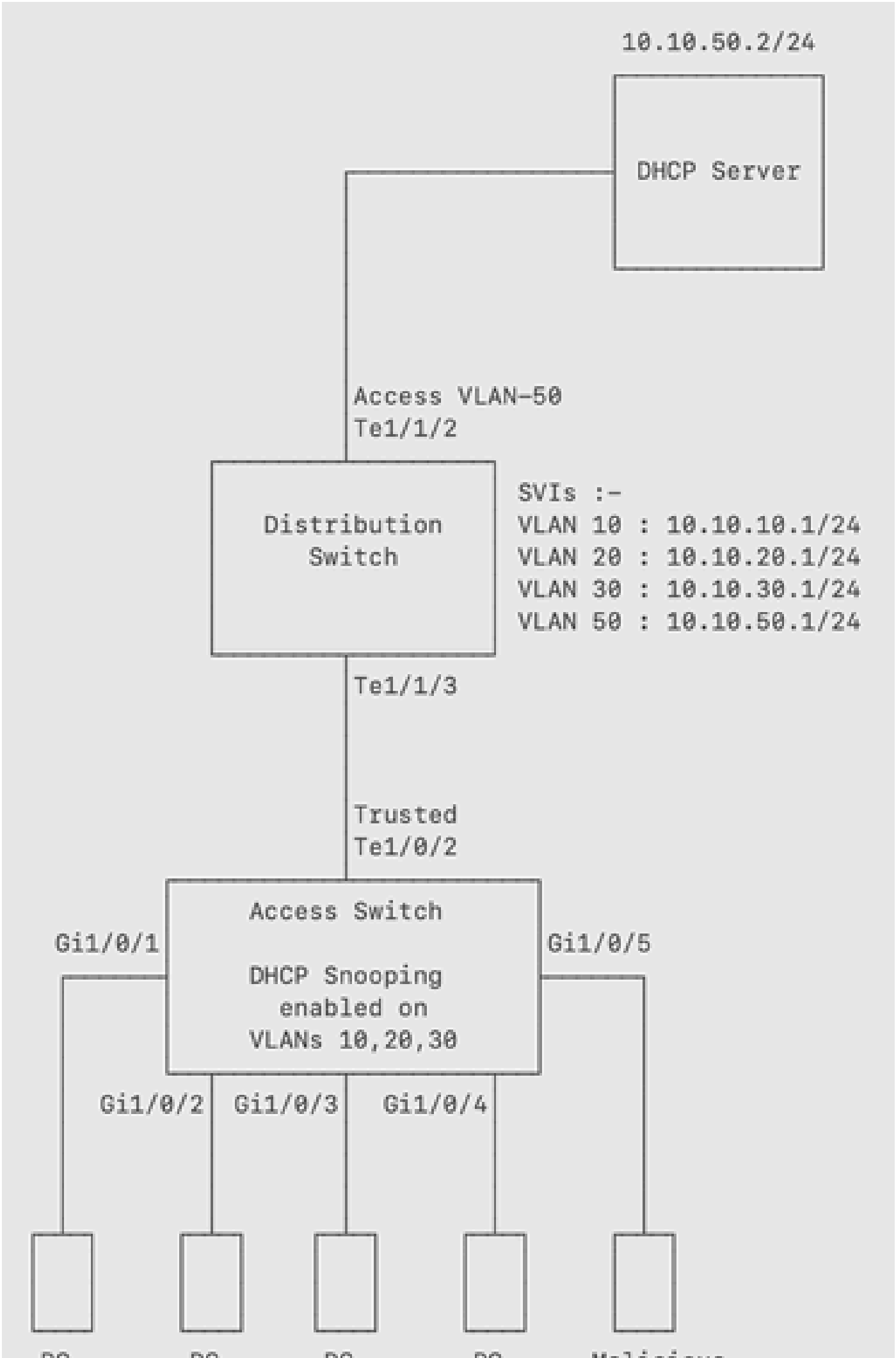



1. By enabling DHCP snooping in the Access Switches, configure the switch to listen in on DHCP traffic and stop any malicious DHCP packets which are received on untrusted ports.
2. As soon as you enable DHCP snooping in the Switch, all interfaces automatically become untrusted.
3. Keep the ports connected to end devices untrusted and configure the ports connected towards the genuine DHCP server as trusted.
4. An untrusted interface will block DHCP offer messages. DHCP offer messages will only be allowed on trusted ports.
5. You can limit the number of DHCP discover packets that end hosts can send to an untrusted interface per

second. This is a security mechanism to safeguard the DHCP server from abnormally high number of incoming DHCP discovers which can exhaust the pool within no time.

In this section, it is explained how to configure DHCP Snooping in a Switched Network:

Topology:


10.10.50.2/24
DHCP Server
Access VLAN-50
Te1/1/2
Distribution Switch
SVIs :-
VLAN 10 : 10.10.10.1/24
VLAN 20 : 10.10.20.1/24
VLAN 30 : 10.10.30.1/24
VLAN 50 : 10.10.50.1/24
Te1/1/3
Trusted
Te1/0/2
Access Switch
DHCP Snooping enabled on VLANs 10,20,30
Gi1/0/1
Gi1/0/5
Gi1/0/2
Gi1/0/3
Gi1/0/4

```
ip dhcp snooping vlan 10,20,30
```

Step 2. Configure DHCP snooping trust on all interface/s of the Access Switch that receive DHCP offers from genuine DHCP server/s. The number of such interfaces depends on the Network design and placement of DHCP servers. These are the interfaces which are going towards the genuine DHCP Server.

Access Switch:

```
interface TenGigabitEthernet1/0/2
switchport mode trunk
ip dhcp snooping trust
```

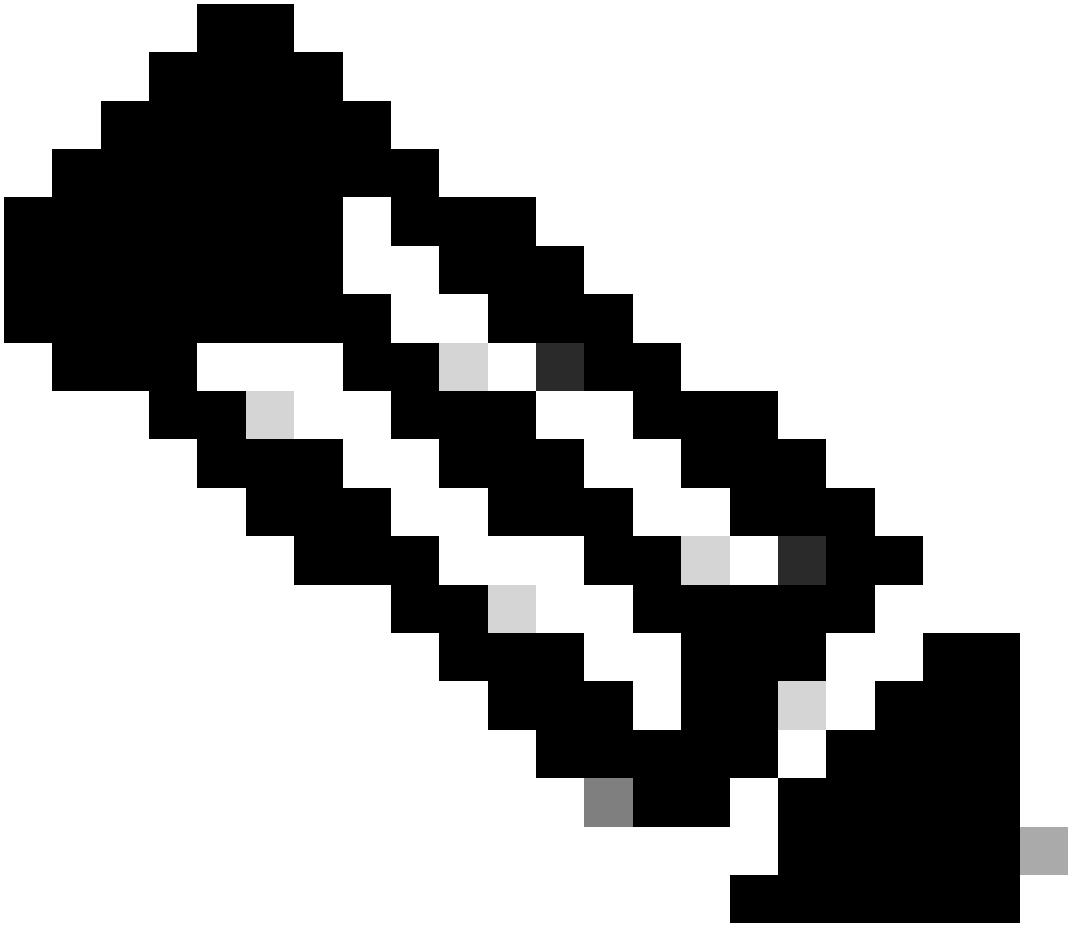
Step 3. Once you configure DHCP snooping globally, all ports in the Switch become untrusted automatically (except the ones which you trust manually, as shown previously). You can however, configure the number of DHCP discover packets that end hosts can send to untrusted interfaces per second.
This is a security mechanism to safeguard the DHCP server from abnormally high number of incoming DHCP discovers which can exhaust the pool within no time.

```
interface range Gi1/0/1-5
ip dhcp snooping limit rate 10
```

Verification:

```
Access_SW#show ip dhcp snooping

Switch DHCP snooping is enabled

Switch DHCP gleaning is disabled

DHCP snooping is configured on following VLANs:

10,20,30

DHCP snooping is operational on following VLANs:

10,20,30

DHCP snooping is configured on the following L3 Interfaces:



Insertion of option 82 is disabled

   circuit-id default format: vlan-mod-port

   remote-id: 00fc.ba9e.3980 (MAC)
```

```
Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:


Interface                  Trusted    Allow option    Rate limit (pps)

-----------------------    -------    ------------    ----------------

GigabitEthernet1/0/1             no         no              10

  Custom circuit-ids:

GigabitEthernet1/0/2             no         no              10

  Custom circuit-ids:

GigabitEthernet1/0/3             no         no              10

  Custom circuit-ids:

GigabitEthernet1/0/4             no         no              10

  Custom circuit-ids:

GigabitEthernet1/0/5             no         no              10

  Custom circuit-ids:

TenGigabitEthernet1/0/2          yes        yes             unlimited

  Custom circuit-ids:
```



**Note**: If you look at this output, you see that Gi1/0/5 which is connected to the Malicious DHCP server is mentioned in the **show ip dhcp snooping** output as untrusted.

So, DHCP Snooping will do all its checks on these ports.
For example, this will cause any incoming DHCP offers on this port (Gi1/0/5) to be dropped.

Here is the DHCP Snooping binding table, showing the IP Address, MAC Address and interface for 3 clients on Gi1/0/1, Gi1/0/2, Gi1/0/3:

```
Access_SW#show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:FC:BA:9E:39:82 10.10.10.2 62488 dhcp-snooping 10 GigabitEthernet1/0/1
00:FC:BA:9E:39:A6 10.10.20.2 62492 dhcp-snooping 20 GigabitEthernet1/0/2
00:FC:BA:9E:39:89 10.10.30.3 62492 dhcp-snooping 30 GigabitEthernet1/0/3
Total number of bindings: 3
```

For demonstration purposes, `ip dhcp snooping trust` config is removed from under Te1/0/2 in the Access Switch. Please take a look at the logs generated in the Switch:

```
Access_SW#sh cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
Dist_SW Ten 1/0/2 175 R S I C9300-48U Ten 1/1/3

Total cdp entries displayed : 1
```

```
Access_SW#show run int Te1/0/2
Building configuration...

Current configuration : 64 bytes
!
interface TenGigabitEthernet1/0/2
switchport mode trunk

*Apr 4 01:12:47.149: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untru
*Apr 4 01:14:07.161: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untru
*Apr 4 01:29:30.634: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untru
*Apr 4 01:30:03.286: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untru
```

- As you can see, the Access Switch is dropping incoming DHCP offer packets on Te1/0/2 since it is no longer trusted.
- The MAC addresses in the logs belong to the SVIs of VLAN 10,20 and 30 since they are the ones sending these offers from the DHCP server to these clients.

# ARP Poisoning

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. It’s a simple protocol but vulnerable to an attack called ARP poisoning.

ARP poisoning is an attack where an attacker sends a fake ARP reply packets on the network.

A malicious user can attack hosts, switches, and routers connected to your 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

This is the classic Man-in-the-middle attack.

# Prevention Mechanisms

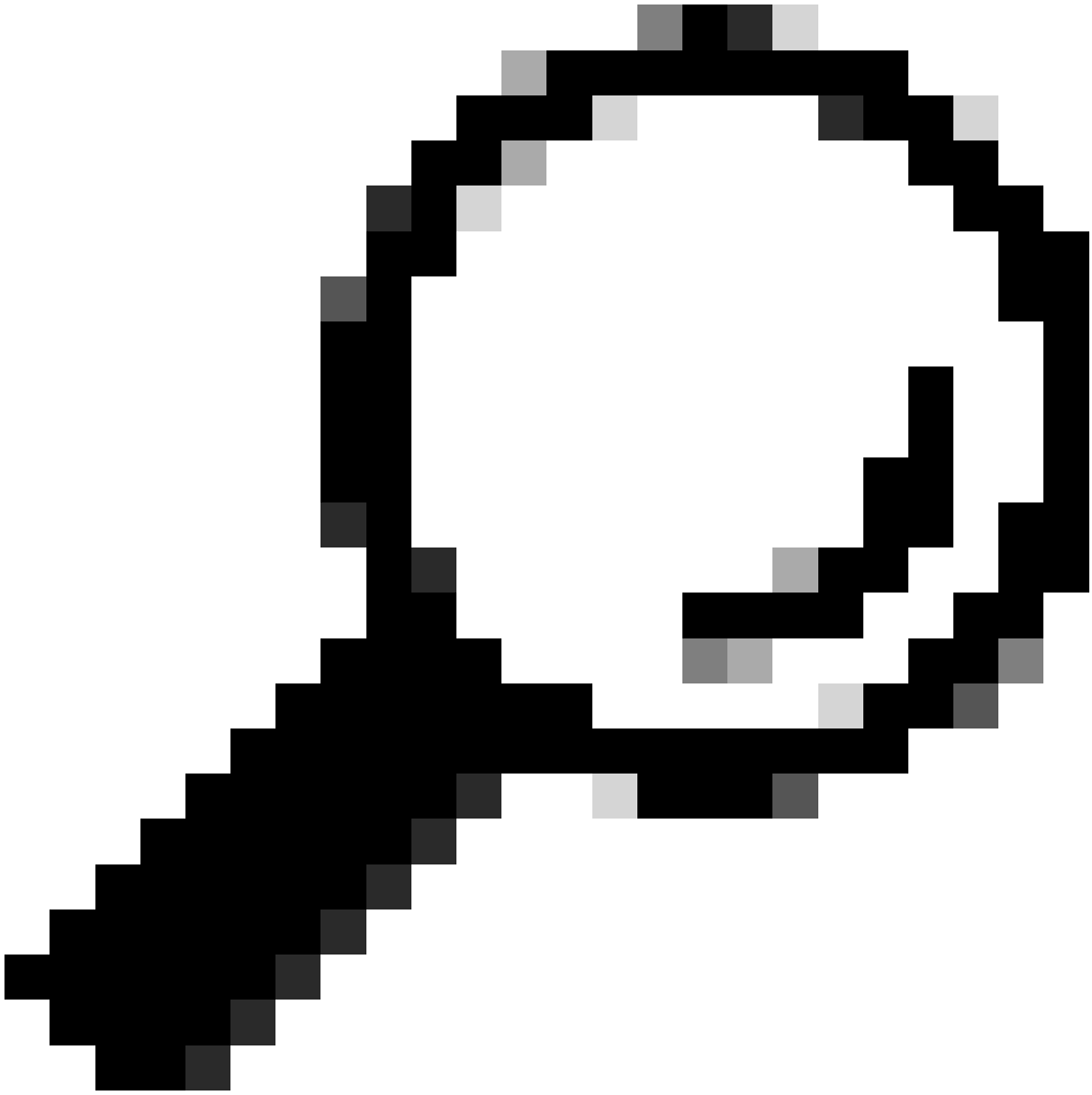
## Dynamic ARP Inspection (DAI)

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

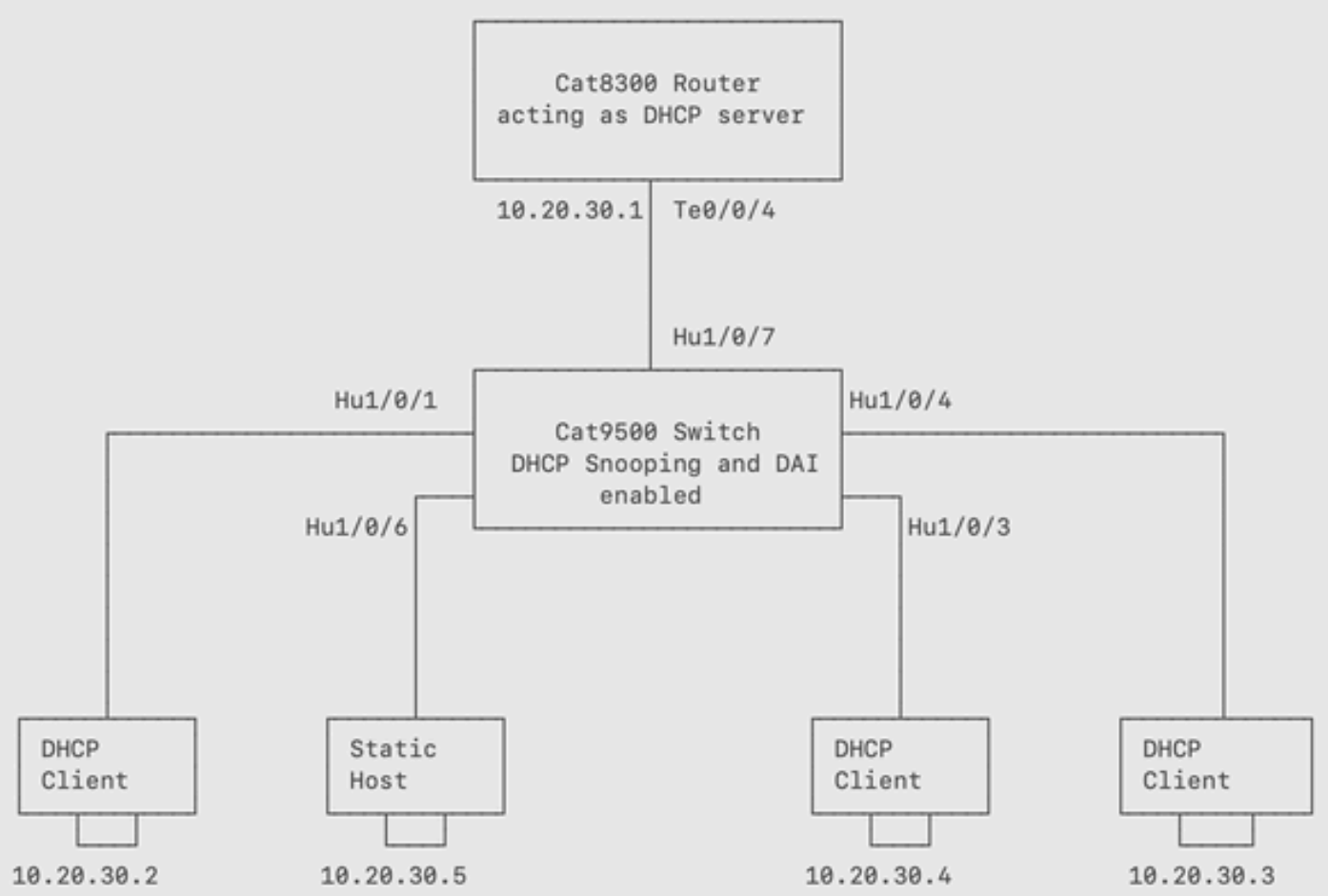
Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- 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

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database.
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.



**Tip**: Refer to https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg/configuring_dynamic_arp_inspection.html




This image demonstartes Cat9500 Switch connected to four hosts, out of which 3 hosts are DHCP clients and 1 host has static IP address (10.20.30.5). The DHCP server is a Cat8300 series router configured with a DHCP pool.

The above topology is used to demonstrate how DAI detects invalid ARP requests on an interface and protects the network from malicious attackers.

Configuration:

Step 1. Configure DHCP snooping and DAI globally in the Switch.

```
F241.24.02-9500-1#sh run | i dhcp
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping
```

```
F241.24.02-9500-1#sh run | i ip arp
ip arp inspection vlan 10
```

Step 2. Configure the interface Hu1/0/7 which is connected to the DHCP server as a trusted port. This will allow the DHCP offers to ingress the interface and subsequently reach the DHCP clients.

```
F241.24.02-9500-1#sh run int Hu1/0/7
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/7
switchport access vlan 10
ip dhcp snooping trust
end
```

Step 3. Configure the ports connected to the DHCP clients as access ports allowing VLAN 10.

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
end
```

```
F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
end
```

Step 4. Verify if the DHCP clients have received IP address from the DHCP server, from the DHCP Snooping binding table in the Cat9500 Switch.

```
F241.24.02-9500-1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
78:72:5D:1B:7F:3F   10.20.30.2       85046       dhcp-snooping   10    HundredGigE1/0/1
5C:71:0D:CD:EE:0C   10.20.30.3       85065       dhcp-snooping   10    HundredGigE1/0/4
2C:4F:52:01:AA:CC   10.20.30.4       85085       dhcp-snooping   10    HundredGigE1/0/3
Total number of bindings: 3
```

You can also check the bindings in the DHCP Server.

```
DHCP_Server#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
10.20.30.2      0063.6973.636f.2d37.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEtherne
                3837.322e.3564.3162.
                2e37.6633.662d.4875.
                312f.302f.31
10.20.30.3      0063.6973.636f.2d35.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEtherne
                6337.312e.3064.6364.
                2e65.6530.632d.5465.
                312f.302f.35
10.20.30.4      0063.6973.636f.2d32.    Apr 08 2024 07:05 AM    Automatic  Active     TenGigabitEtherne
                6334.662e.3532.3031.
                2e61.6163.632d.5465.
                312f.302f.35
```

Step 5: Change the IP Address of the host connected to Hu1/0/6 from 10.20.30.5 to 10.20.30.2 and try to ping the other DHCP clients from that host.

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.....
```

These invalid ARP logs can be see on the Cat9500 Switch:

```
F241.24.02-9500-1#
*Apr 7 09:29:24.520: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:26.520: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:28.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:30.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:32.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
F241.24.02-9500-1#
*Apr 7 09:29:47.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:49.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:51.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:53.522: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
*Apr 7 09:29:55.523: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956
```

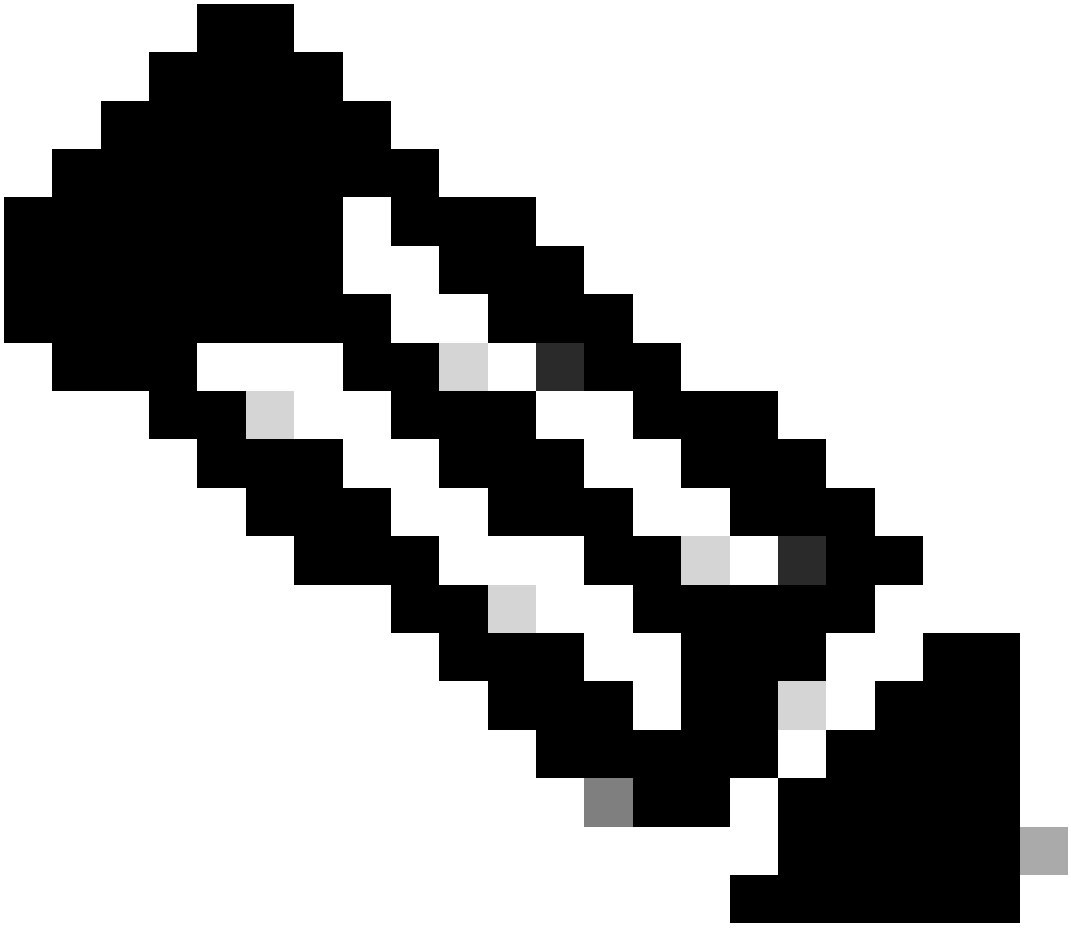
- As you can see, when you try to ping 10.20.30.3 and 10.20.30.4 from the Static_Host, you are not able to do so.
  Even though Static_Host tried to spoof the IP address of the legit DHCP client, it was not able to do so because any ARP packet that arrives on Hu1/0/6 will be inspected by the Switch and compared with the data present in the DHCP snooping binding table.
- The subsequent logs from the Cat9500 Switch confirms that the ARP requests being sent from the Static_Host to the DHCP clients are being dropped.
- The Cat9500 Switch achieves this by referring the DHCP snooping binding database.
- When an ARP request ingresses Hu1/0/6 with the source MAC-IP which does not match the values present in the DHCP snooping binding database, the Switch will drop the ARP request.

Step 6. Verification:

```
F241.24.02-9500-1#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


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


Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
----      ---------        -------     ----------      ---------
   10              9             39             39              0


Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
----   ------------    -----------  -------------   -------------------
   10              6              3              0                     0


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

In this output, you can see the number of packets dropped and allowed by DAI in VLAN 10 in the Cat9500 Switch.



**Note**: One very important scenario could be a legit host in the Network who has a Static IP Address (E.g. 10.20.30.5) address assigned to it?

Though the host is not trying to spoof anything, it will still be isolated from the Network because its MAC-IP binding data is not present in the DHCP snooping binding database.

This is because the Static Host never used DHCP to receive the IP Address, since it was statically assigned to it.

We have a few workarounds that can be implemented to provide connectivity to legit hosts who have Static IP Addresses.

---

Option 1.

Configure the interface connected to the host with ip arp inspection trust.

```
F241.24.02-9500-1#sh run int HundredGigE 1/0/6
Building configuration...
```

```
Current configuration : 110 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
switchport mode access
ip arp inspection trust
end
```

```
Static_Host#ping 10.20.30.4
*Apr 7 18:44:45.299 JST: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.1.5)
F241.24.02-9300-STACK#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Option 2.

Allow the Static Host by using an ARP Access-List:

```
F241.24.02-9500-1#sh run | s arp access-list
arp access-list DAI
permit ip host 10.20.30.5 mac host 7035.0956.7ee4

F241.24.02-9500-1#sh run | i ip arp ins
ip arp inspection filter DAI vlan 10
```

```
Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Option 3.

Configure a binding table entry for the Static Host.

```
F241.24.02-9500-1#sh run | i binding
ip source binding 7035.0956.7EE4 vlan 10 10.20.30.5 interface Hu1/0/6
```

```
F241.24.02-9500-1#show ip source binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 80640 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 80659 dhcp-snooping 10 HundredGigE1/0/4
70:35:09:56:7E:E4 10.20.30.5 infinite static 10 HundredGigE1/0/6
2C:4F:52:01:AA:CC 10.20.30.4 80679 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 4
```

```
Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

```
Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Additional options available with DAI:

```
F241.24.02-9500-1(config)#ip arp inspection validate ?
dst-mac Validate destination MAC address
ip Validate IP addresses
src-mac Validate source MAC address
```

For src-mac, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped

For dst-mac, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For IP, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

You can also configure ARP rate-limiting. By default, there is a limit of 15 pps for ARP traffic on untrusted interfaces:

```
Switch(config)#interface Gigabitethernet<>
Switch(config-if)#ip arp inspection limit rate 10
```

## IP Source Guard

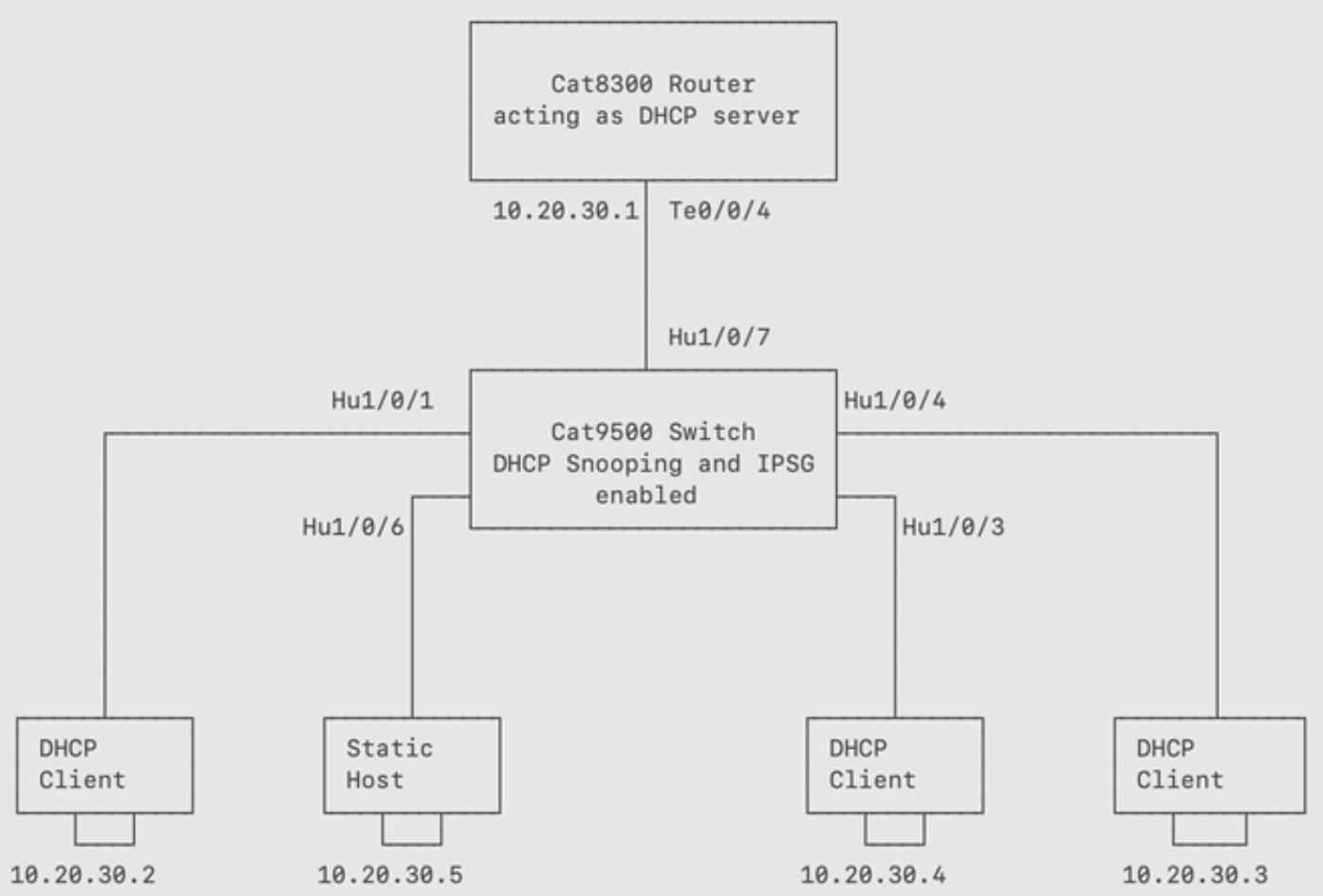
- IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and manually configured IP source bindings.
- You can use IPSG to prevent traffic attacks if a host tries to use the IP address of its neighbor.
- You can enable IPSG when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.
- The switch uses a source IP lookup table in hardware to bind IP addresses to ports. For IP and MAC filtering, a combination of source IP and source MAC lookups are used. IP traffic with a source IP address in the binding table is allowed, all other traffic is denied.
- The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when the IP source guard is enabled.
- You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

### IPSG for Static Hosts

- IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port.

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg/configuring_ip_source_guard.html




Cat9500 Switch is connected to four hosts out of which 3 hosts are DHCP clients and 1 host has a static IP address. The DHCP server is a Cat8300 series router configured with a DHCP pool.
You can use this topology to demonstrate how IPSG detects and blocks traffic from hosts whose MAC-IP bindings are not present in the DHCP snooping binding database.

Configure:

Step 1. Configure DHCP snooping globally in the Cat9500 Switch.

```
F241.24.02-9500-1#sh run | i dhcp
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip dhcp snooping
```

Step 2. Configure the interface Te1/0/7 which is connected to the DHCP server as a trusted port. This allows the DHCP offers to ingress the interface and subsequently reach the DHCP clients.

```
F241.24.02-9500-1#sh run int Hu1/0/7
```

```
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/7
switchport access vlan 10
ip dhcp snooping trust
end
```

Step 3. Configure the ports connected to the DHCP clients as access ports allowing VLAN 10.

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 61 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 85 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
end
```

Step 4. Verify if the DHCP clients have received the IP address from the DHCP server.

```
F241.24.02-9500-1#sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 85046 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 85065 dhcp-snooping 10 HundredGigE1/0/4
```

```
2C:4F:52:01:AA:CC 10.20.30.4 85085 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 3



F241.24.02-9500-1#show ip source binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
78:72:5D:1B:7F:3F 10.20.30.2 64764 dhcp-snooping 10 HundredGigE1/0/1
5C:71:0D:CD:EE:0C 10.20.30.3 64783 dhcp-snooping 10 HundredGigE1/0/4
2C:4F:52:01:AA:CC 10.20.30.4 64803 dhcp-snooping 10 HundredGigE1/0/3
Total number of bindings: 3



DHCP_Server#show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address      Client-ID/              Lease expiration        Type       State      Interface

                Hardware address/

                User name

10.20.30.2      0063.6973.636f.2d37.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEtherne

                3837.322e.3564.3162.

                2e37.6633.662d.4875.

                312f.302f.31

10.20.30.3      0063.6973.636f.2d35.    Apr 08 2024 07:04 AM    Automatic  Active     TenGigabitEtherne

                6337.312e.3064.6364.

                2e65.6530.632d.5465.

                312f.302f.35

10.20.30.4      0063.6973.636f.2d32.    Apr 08 2024 07:05 AM    Automatic  Active     TenGigabitEtherne

                6334.662e.3532.3031.

                2e61.6163.632d.5465.

                312f.302f.35
```

Step 5. Configure IPSG under the interfaces connected to all the end hosts (3x DHCP clients and 1x host with static IP address).

```
F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 79 bytes
```

```
!
interface HundredGigE1/0/3
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 79 bytes
!
interface HundredGigE1/0/4
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 79 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
ip verify source
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 103 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
ip verify source
end
```

Verification:

```
F241.24.02-9500-1#show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan

---------  -----------  -----------  ---------------  -----------------  ----

Hu1/0/1    ip           active       10.20.30.2                          10

Hu1/0/3    ip           active       10.20.30.4                          10

Hu1/0/4    ip           active       10.20.30.3                          10

Hu1/0/6    ip           active       deny-all                            10
```

From this output, you can see the IP Address field is set to deny-all for Hu1/0/6 because there is no MAC-IP binding corresponding to this interface in the DHCP snooping binding table.

Step 6. Try to ping the DHCP clients with IP addresses 10.20.30.2, 10.20.30.3 and 10.20.30.4 from the Static_Host.

```
Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
.....
```

```
F241.24.02-9500-1(config)# ip source binding <mac-address-of-static-host> vlan 10 10.20.30.5 interface
```

```
F241.24.02-9500-1#show run int Hu1/0/6

*Apr  7 15:13:48.449: %SYS-5-CONFIG_I: Configured from console by console

F241.24.02-9500-1#show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan

---------  -----------  -----------  ---------------  -----------------  ----

Hu1/0/1    ip           active       10.20.30.2                          10

Hu1/0/3    ip           active       10.20.30.4                          10

Hu1/0/4    ip           active       10.20.30.3                          10

Hu1/0/6    ip           active       10.20.30.5                          10
```

```
F241.24.02-9500-1#show ip source binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface

------------------  ---------------  ----------  -------------  ----  --------------------

78:72:5D:1B:7F:3F   10.20.30.2       62482       dhcp-snooping   10    HundredGigE1/0/1

5C:71:0D:CD:EE:0C   10.20.30.3       62501       dhcp-snooping   10    HundredGigE1/0/4
```

```
70:35:09:56:7E:E4   10.20.30.5       infinite    static          10    HundredGigE1/0/6

2C:4F:52:01:AA:CC   10.20.30.4       62521       dhcp-snooping   10    HundredGigE1/0/3

Total number of bindings: 4
```

```
Verification:

Static_Host#ping 10.20.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Static_Host#ping 10.20.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.30.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Additional options available with IPSG:

By default, IPSG filters incoming traffic on untrusted ports based on only IP addresses.
If you want to perform the filtering based on both IP and MAC address, perform these steps.

```
F241.24.02-9500-1#sh run int Hu1/0/1
Building configuration...

Current configuration : 89 bytes
!
interface HundredGigE1/0/1
switchport access vlan 10
ip verify source mac-check
end

F241.24.02-9500-1#sh run int Hu1/0/3
Building configuration...

Current configuration : 89 bytes
!
interface HundredGigE1/0/3
switchport access vlan 10
ip verify source mac-check
end

F241.24.02-9500-1#sh run int Hu1/0/4
Building configuration...

Current configuration : 89 bytes
```

```
!
interface HundredGigE1/0/4
switchport access vlan 10
ip verify source mac-check
end

F241.24.02-9500-1#sh run int Hu1/0/6
Building configuration...

Current configuration : 113 bytes
!
interface HundredGigE1/0/6
switchport access vlan 10
switchport mode access
ip verify source mac-check
end
```

```
F241.24.02-9500-1#show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan

---------  -----------  -----------  ---------------  -----------------  ----

Hu1/0/1    ip-mac       active       10.20.30.2       78:72:5D:1B:7F:3F   10

Hu1/0/3    ip-mac       active       10.20.30.4       2C:4F:52:01:AA:CC   10

Hu1/0/4    ip-mac       active       10.20.30.3       5C:71:0D:CD:EE:0C   10

Hu1/0/6    ip-mac       active       deny-all         deny-all            10
```

In this output, you can see that the Filter-type is ip-mac. So, the Switch now filters the incoming packets on these interfaces based on both source IP and MAC address.

# Troubleshooting Tips for DAI and IPSG

- The first thing to check while troubleshooting DAI and IPSG-related issues is to verify if the DHCP snooping binding table has been populated correctly.
- Before enabling these features, handle the endpoints with static IP addresses. If you don’t want these devices to lose reachability, please configure static bindings or employ one of the previously mentioned methodologies to make the Switch trust these endpoints.
- While configuring DAI or IPSG in an environment where DHCP snooping is not already enabled and clients have already received IPs from the DHCP server, first enable DHCP snooping and perform either of the two steps:
    - Bounce the client-connected interfaces so that they renew their lease.
    - Wait for the clients to automatically renew their lease. This can take more time but saves you the hassle of manually bouncing all the client-connected ports.

- Performing either of the two steps above will trigger a new DORA transaction. The Switch will sniff the DORA packets and update the binding table. If this is not done and DAI or IPSG is immediately enabled after configuring DHCP snooping, you might land into an issue where all DHCP clients in the Network lose connectivity to the Network.

- While troubleshooting connectivity issues in an environment where DAI or IPSG is configured, ensure that the DHCP snooping binding table is not corrupted. Ensure that the Switch can access the data structure where this table is stored.
- There might be instances where the binding table is exported to a media which takes time to get initialized after the switch boots up or becomes inaccessible to the switch due to some reason. You might have observed connectivity issues in such scenarios.