Catalyst 스위치에서 DAI(Dynamic ARP Inspection) 및 IPSG(IP Source Guard) 문제 해결

목차

소개

이 문서에서는 DAI(Dynamic ARP Inspection) 및 IPSG(IP Source Guard)의 작동 방식과 Catalyst 9K 스위치에서 이를 검증하는 방법에 대해 설명합니다.

DHCP 스누핑 및 관련 기능

DAI와 IPSG로 들어가기 전에 DAI와 IPSG의 전제 조건인 DHCP Snooping에 대해 간략하게 설명해야 합니다.

DHCP(Dynamic Host Configuration Protocol)는 IP(인터넷 프로토콜) 호스트에 해당 IP 주소 및 서브넷 마스크, 기본 게이트웨이 등 기타 관련 구성 정보를 자동으로 제공하는 클라이언트/서버 프로토콜입니다. RFC 2131 및 2132는 DHCP가 많은 구현 세부 정보를 공유하는 프로토콜인 BOOTP(Bootstrap Protocol)를 기반으로 DHCP를 IETF(Internet Engineering Task Force) 표준으로 정의합니다. DHCP를 사용하면 호스트가 DHCP 서버에서 필요한 TCP/IP 컨피그레이션 정보를 얻을 수 있습니다.

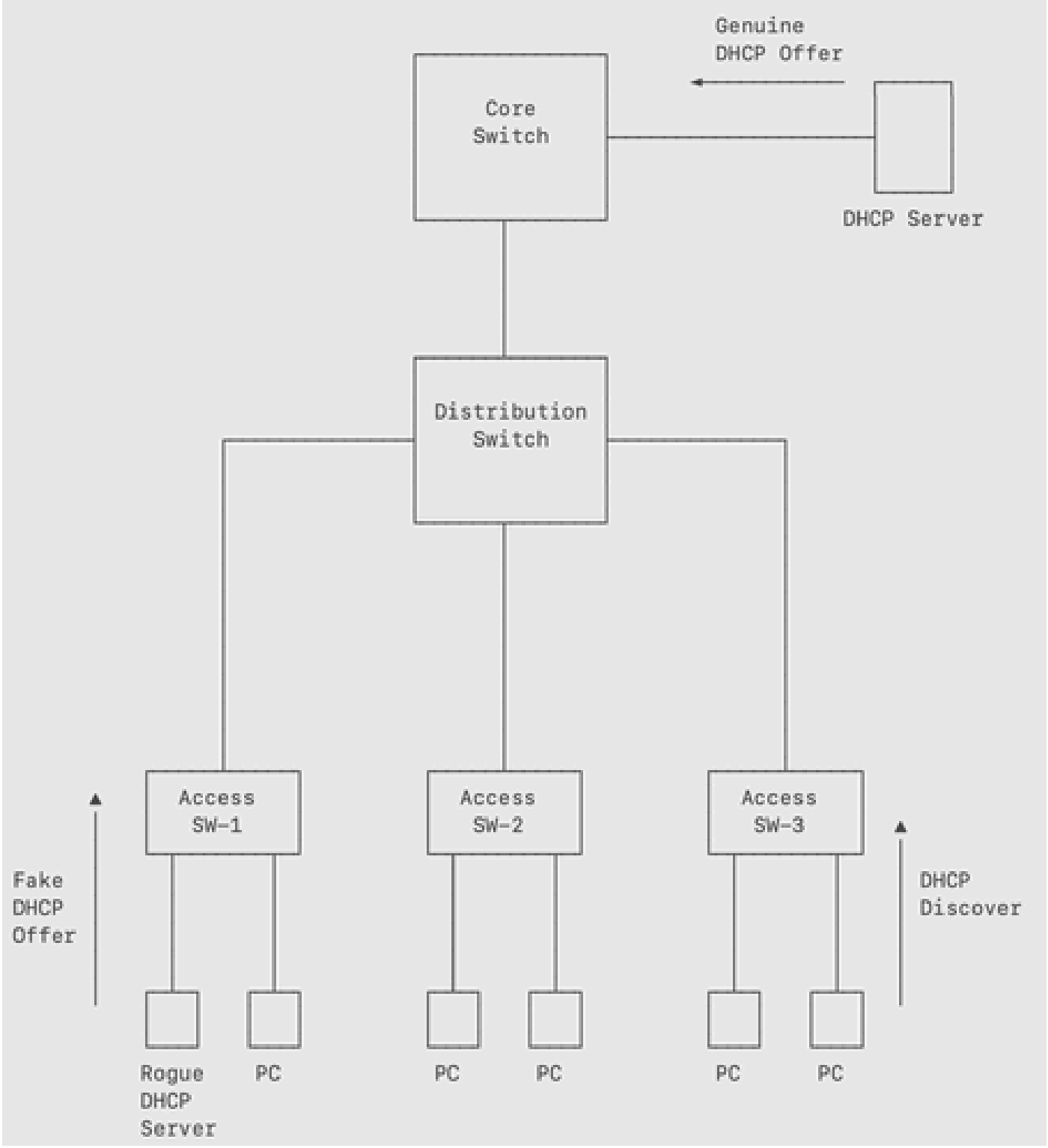
DHCP 스누핑은 신뢰할 수 없는 호스트와 신뢰할 수 있는 DHCP 서버 간의 방화벽 역할을 하는 보안 기능입니다. DHCP 스누핑 기능은 다음 작업을 수행합니다.

- 신뢰할 수 없는 소스에서 수신된 DHCP 메시지를 검증하고 잘못된 메시지를 필터링합니다.
- 속도 - 신뢰할 수 있는 소스와 신뢰할 수 없는 소스의 DHCP 트래픽을 제한합니다.
- 임대 IP 주소가 있는 신뢰할 수 없는 호스트에 대한 정보를 포함하는 DHCP 스누핑 바인딩 데이터베이스를 구축하고 유지 관리합니다.
- DHCP 스누핑 바인딩 데이터베이스를 사용하여 신뢰할 수 없는 호스트의 후속 요청을 검증합니다.

DAI는 네트워크의 ARP(Address Resolution Protocol) 패킷을 검증하는 보안 기능입니다. DAI를 사용하면 네트워크 관리자가 유효하지 않은 MAC 주소가 있는 ARP 패킷을 IP 주소 바인딩에 가로채고 기록하고 폐기할 수 있습니다. 이 기능은 특정 "중간자" 공격으로부터 네트워크를 보호합니다.

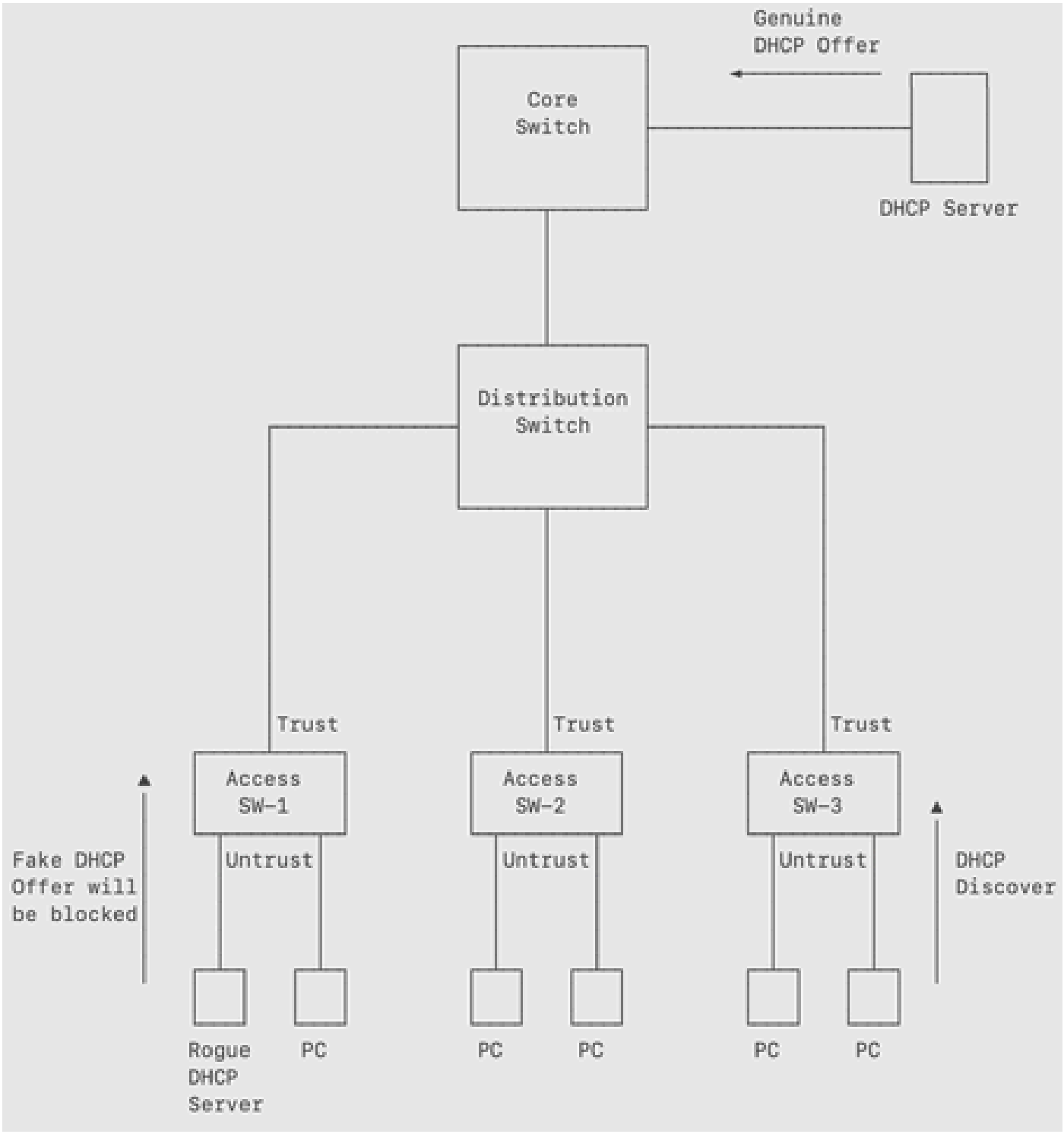
IPSG는 DHCP 스누핑 바인딩 데이터베이스 및 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하여 라우팅되지 않은 레이어 2 인터페이스의 IP 트래픽을 제한하는 보안 기능입니다. 호스트가 인접 디바이스의 IP 주소를 사용하려고 할 경우 IPSG를 사용하여 트래픽 공격을 방지할 수 있습니다.

DHCP 스누핑 없는 시나리오



1. 이 다이어그램에서는 여러 클라이언트가 코어 스위치에 연결된 DHCP 서버에서 IP 주소를 수신하려는 것을 볼 수 있습니다.
2. 그러나 액세스 레이어 스위치 중 하나에 연결된 악성/비인가 DHCP 서버가 있습니다. 이 스위치는 DHCP를 검색하고 실제 DHCP 서버보다 더 빠르게 DHCP 오퍼를 전송할 수 있습니다.
3. 공격자는 클라이언트로부터 모든 트래픽을 수신할 수 있도록 오퍼 메시지에 게이트웨이 주소를 설정하여 통신의 기밀성을 침해할 수 있습니다.
4. 이 사람은 중간자 공격자로 알려져 있어.

DHCP 스누핑 시나리오

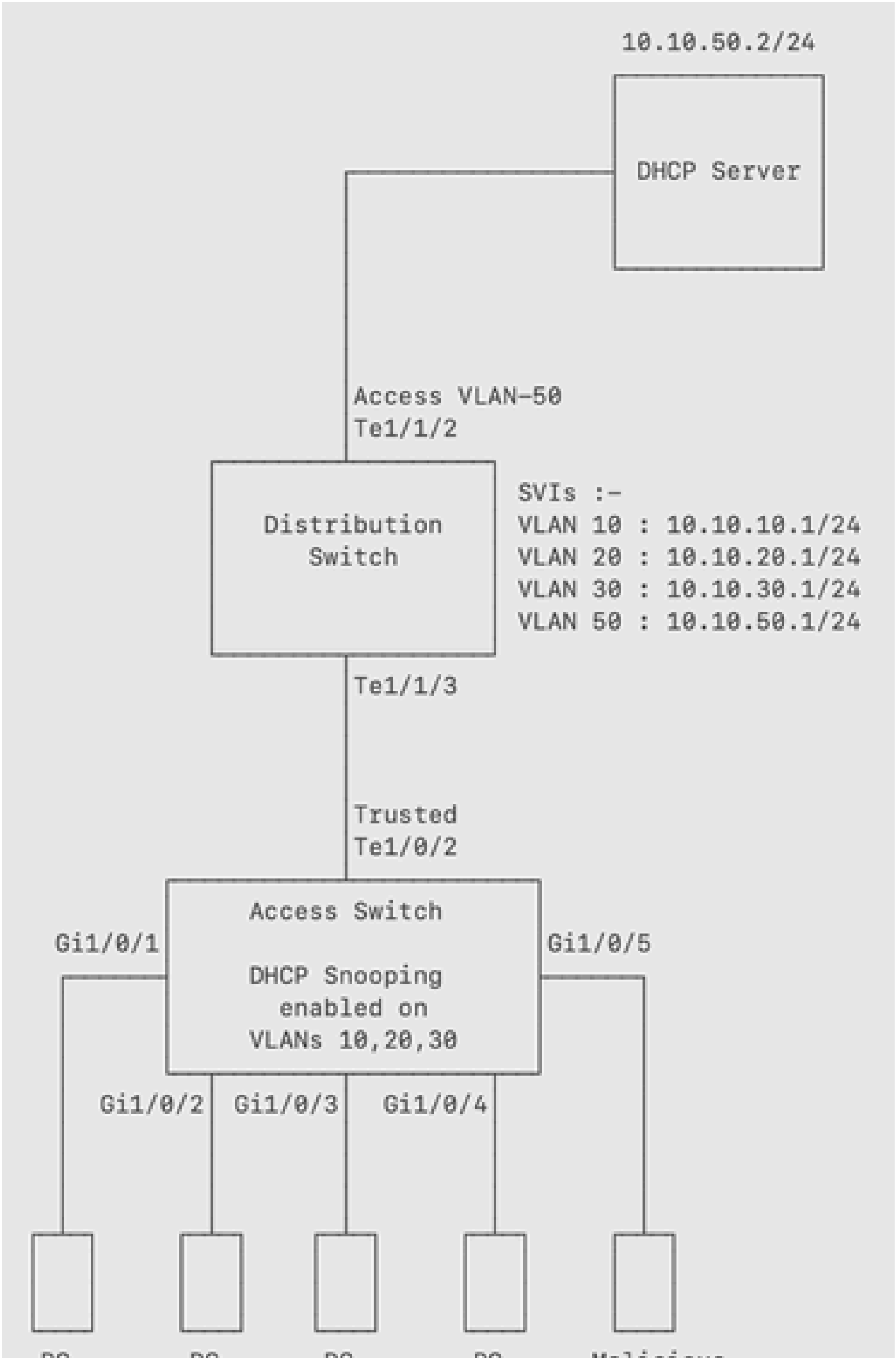


1. 액세스 스위치에서 DHCP 스누핑을 활성화하여 DHCP 트래픽에서 수신 대기하도록 스위치를 구성하고 신뢰할 수 없는 포트에서 수신되는 모든 악성 DHCP 패킷을 중지합니다.
2. 스위치에서 DHCP 스누핑을 활성화하면 모든 인터페이스가 자동으로 신뢰할 수 없게 됩니다.
3. 포트가 최종 장치에 연결되지 않도록 하고 정품 DHCP 서버에 연결된 포트를 신뢰할 수 있도록 구성합니다.
4. 신뢰할 수 없는 인터페이스는 DHCP 오퍼 메시지를 차단합니다. DHCP 제안 메시지는 신뢰할 수 있는 포트에서만 허용됩니다.
5. 종단 호스트가 신뢰할 수 없는 인터페이스로 보낼 수 있는 초당 DHCP 검색 패킷의 수를 제한할

수 있습니다. 이는 DHCP 서버를 비정상적으로 많은 수신 DHCP 검색으로부터 보호하기 위한 보안 메커니즘으로, 빠른 시간 내에 풀을 소진할 수 있습니다.

이 섹션에서는 스위치드 네트워크에서 DHCP 스누핑을 구성하는 방법에 대해 설명합니다.

토폴로지:


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
```

2단계. 정품 DHCP 서버에서 DHCP 제안을 받는 액세스 스위치의 모든 인터페이스에 DHCP 스누핑 트러스트를 구성합니다. 이러한 인터페이스의 수는 네트워크 설계 및 DHCP 서버의 배치에 따라 달라집니다. 이러한 인터페이스는 정품 DHCP 서버로 전송됩니다.

액세스 스위치:

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

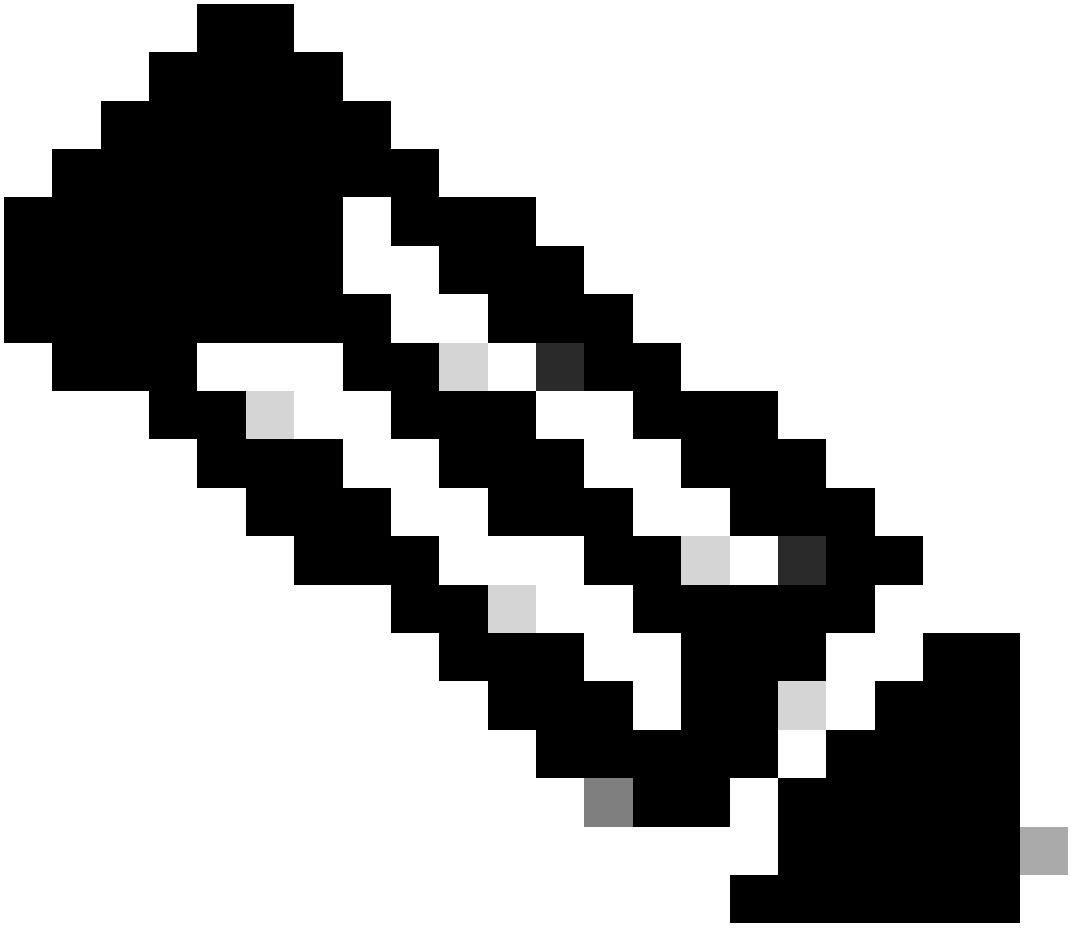
3단계. DHCP 스누핑을 전역으로 구성하면 스위치의 모든 포트는 자동으로 신뢰 해제됩니다(앞서 설명한 것처럼 수동으로 신뢰하는 포트는 제외). 그러나 종단 호스트가 신뢰할 수 없는 인터페이스에 초당 전송할 수 있는 DHCP 검색 패킷의 수를 구성할 수 있습니다.
이는 DHCP 서버를 비정상적으로 많은 수신 DHCP 검색으로부터 보호하기 위한 보안 메커니즘으로, 빠른 시간 내에 풀을 소진할 수 있습니다.

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

확인:

```
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:
```



참고: 이 출력을 보면 Malicious DHCP 서버에 연결된 Gi1/0/5가 출력에 신뢰할 수 없는 **show ip dhcp snooping** 것으로 언급되어 있습니다.

따라서 DHCP Snooping은 이러한 포트에 대한 모든 검사를 수행합니다.
예를 들어, 이렇게 하면 이 포트(Gi1/0/5)에서 들어오는 모든 DHCP 오퍼가 삭제됩니다.

다음은 Gi1/0/1, Gi1/0/2, Gi1/0/3의 3개 클라이언트에 대한 IP 주소, MAC 주소 및 인터페이스를 보여주는 DHCP 스누핑 바인딩 테이블입니다.

```
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

데모용으로 ip dhcp snooping trust Access Switch의 Te1/0/2에서 컨피그레이션이 제거됩니다. 스위치에서 생성된 로그를 확인하십시오.

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 untrusted port, message
*Apr 4 01:14:07.161: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message
*Apr 4 01:29:30.634: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message
*Apr 4 01:30:03.286: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message

- 보시다시피 액세스 스위치는 더 이상 신뢰할 수 없으므로 Te1/0/2에서 수신 DHCP 제공 패킷을 삭제합니다.
- 로그의 MAC 주소는 VLAN 10, 20 및 30의 SVI에 속합니다. DHCP 서버에서 이러한 클라이언트로 이러한 제안을 전송하기 때문입니다.

ARP 중독

ARP는 IP 주소를 MAC 주소에 매핑하여 레이어 2 브로드캐스트 도메인 내에서 IP 통신을 제공합니다. 이 프로토콜은 간단하지만 ARP 포이즈닝이라는 공격에 취약합니다.

ARP 포이즈닝은 공격자가 네트워크에서 가짜 ARP 응답 패킷을 전송하는 공격입니다.

악의적인 사용자는 서브넷에 연결된 시스템의 ARP 캐시를 피독하고 서브넷의 다른 호스트에 대한 트래픽을 차단하여 레이어 2 네트워크에 연결된 호스트, 스위치 및 라우터를 공격할 수 있습니다

이건 전형적인 중간자 공격입니다.

방지 메커니즘

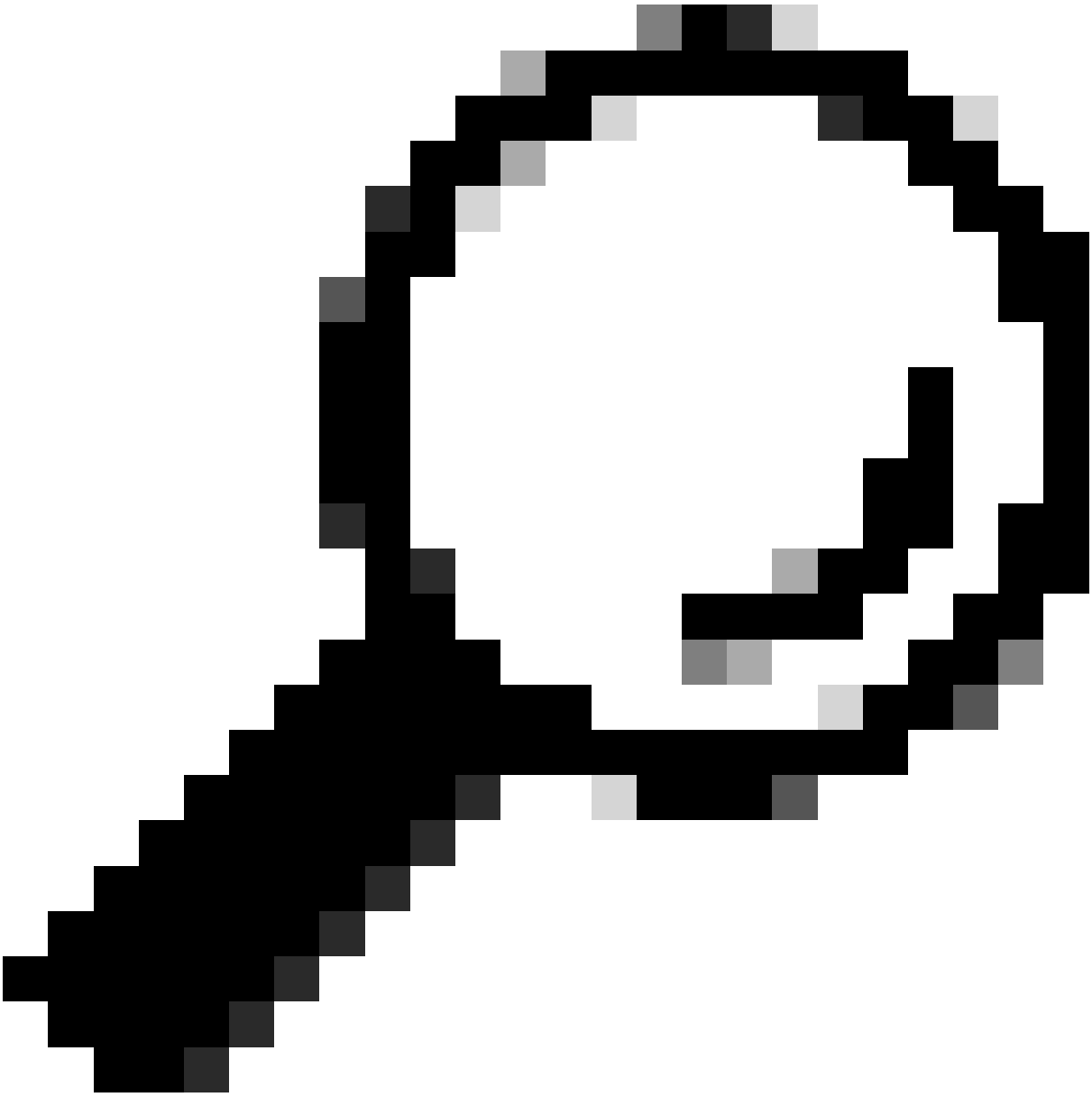
동적 ARP 검사(DAI)

동적 ARP 검사는 네트워크의 ARP 패킷을 검증하는 보안 기능입니다. 유효하지 않은 IP-MAC 주소 바인딩이 있는 ARP 패킷을 가로채고 로깅하고 폐기합니다. 이 기능은 특정 중간자 공격으로부터 네트워크를 보호합니다.

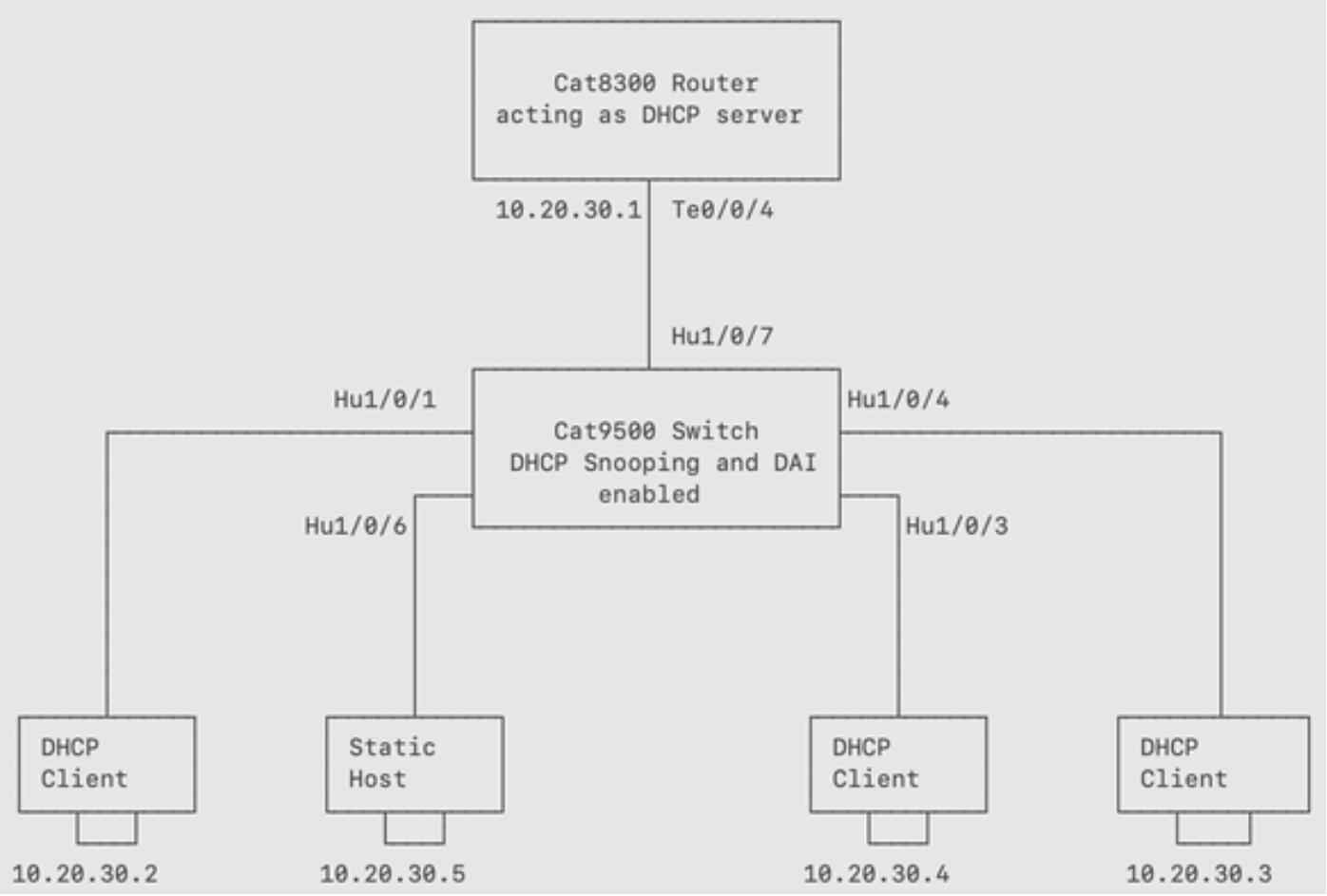
동적 ARP 검사에서는 유효한 ARP 요청 및 응답만 릴레이됩니다. 스위치는 다음 작업을 수행합니다.

- 신뢰할 수 없는 포트에서 모든 ARP 요청 및 응답 가로채기
- 로컬 ARP 캐시를 업데이트하기 전 또는 적절한 대상에 패킷을 전달하기 전에 이러한 인터셉트된 각 패킷에 유효한 IP-MAC 주소 바인딩이 있는지 확인합니다
- 유효하지 않은 ARP 패킷을 삭제합니다.

동적 ARP 검사는 신뢰할 수 있는 데이터베이스인 DHCP 스누핑 바인딩 데이터베이스에 저장된 유효한 IP-MAC 주소 바인딩을 기반으로 ARP 패킷의 유효성을 확인합니다.
이 데이터베이스는 VLAN 및 스위치에서 DHCP 스누핑이 활성화된 경우 DHCP 스누핑에 의해 구축됩니다. ARP 패킷이 신뢰할 수 있는 인터페이스에서 수신되면 스위치는 확인 없이 패킷을 전달합니다.
신뢰할 수 없는 인터페이스에서는 유효한 경우에만 스위치가 패킷을 전달합니다.



팁: 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.html을 참조하십시오.



이 이미지는 4개의 호스트에 연결된 Cat9500 Switch를 보여줍니다. 이 중 3개의 호스트는 DHCP 클라이언트이고 1개의 호스트는 고정 IP 주소(10.20.30.5)를 갖습니다. DHCP 서버는 DHCP 풀로 구성된 Cat8300 시리즈 라우터입니다.

위 토폴로지는 DAI가 인터페이스에서 유효하지 않은 ARP 요청을 탐지하고 악의적인 공격자로부터 네트워크를 보호하는 방법을 보여 주는 데 사용됩니다.

설정:

1단계. 스위치에서 DHCP 스누핑 및 DAI를 전역적으로 구성합니다.

```
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
```

2단계. DHCP 서버에 트러스트된 포트로 연결된 인터페이스 Hu1/0/7을 구성합니다. 이렇게 하면 DHCP 오퍼가 인터페이스를 인그레스(ingress)하고 DHCP 클라이언트에 도달할 수 있습니다.

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

3단계. DHCP 클라이언트에 연결된 포트를 VLAN 10을 허용하는 액세스 포트로 구성합니다.

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

4단계. DHCP 클라이언트가 DHCP 서버의 IP 주소를 받았는지, Cat9500 스위치의 DHCP Snooping 바인딩 테이블에서 받았는지 확인합니다.

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

DHCP 서버에서 바인딩을 확인할 수도 있습니다.

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 TenGigabitEthernet0/0/4

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 TenGigabitEthernet0/0/4

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 TenGigabitEthernet0/0/4

6334.662e.3532.3031.

2e61.6163.632d.5465.

312f.302f.35

5단계: Hu1/0/6에 연결된 호스트의 IP 주소를 10.20.30.5에서 10.20.30.2로 변경하고 해당 호스트에서 다른 DHCP 클라이언트를 ping해 봅니다.

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:
.....

Cat9500 스위치에서 다음과 같은 잘못된 ARP 로그를 볼 수 있습니다.

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.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:26.520: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:28.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:30.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:32.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
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.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:49.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:51.521: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:53.522: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*Apr 7 09:29:55.523: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Hu1/0/6, vlan 10.([7035.0956.7ee4/10.20.30.2/0000.0000.0000

- 보시다시피 Static_Host에서 10.20.30.3 및 10.20.30.4를 ping하려고 하면 ping을 수행할 수 없습니다.
  Static_Host가 정상 DHCP 클라이언트의 IP 주소를 스푸핑하려고 했지만, Hu1/0/6에 도착하는 모든 ARP 패킷이 스위치에 의해 검사되고 DHCP 스누핑 바인딩 테이블에 존재하는 데이터와 비교되기 때문에 스푸핑할 수 없었습니다.

- Cat9500 스위치의 후속 로그는 Static_Host에서 DHCP 클라이언트로 전송되는 ARP 요청이 삭제됨을 확인합니다.

- Cat9500 스위치는 DHCP 스누핑 바인딩 데이터베이스를 참조하여 이를 실현합니다.

- ARP 요청이 DHCP 스누핑 바인딩 데이터베이스에 있는 값과 일치하지 않는 소스 MAC-IP를 사용하여 Hu1/0/6을 인그레스할 때 스위치는 ARP 요청을 삭제합니다.

6단계. 확인:

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

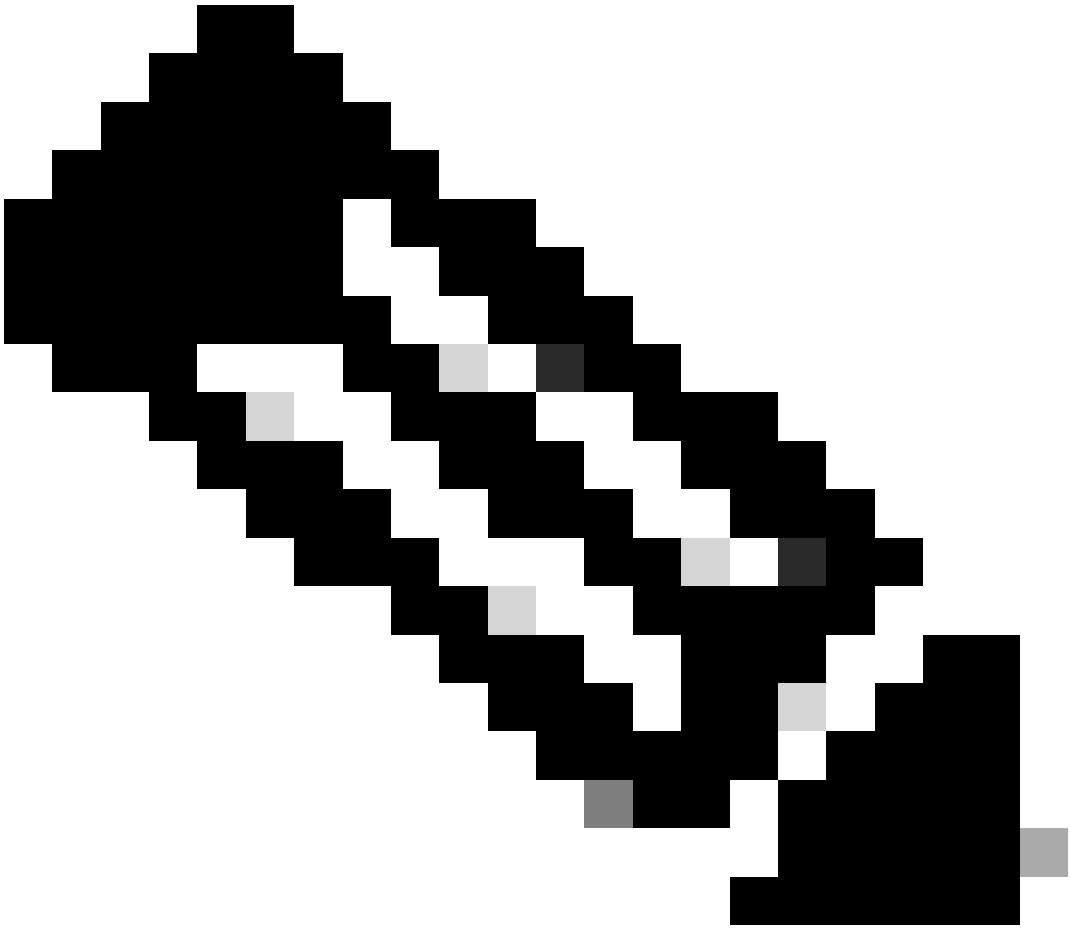
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
10	9	39	39	0

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

이 출력에서는 Cat9500 스위치의 VLAN 10에서 DAI가 삭제하고 허용하는 패킷 수를 확인할 수 있습니다.



참고: 매우 중요한 시나리오 중 하나는 고정 IP 주소(예: 10.20.30.5)가 할당된 올바른 네트워크 호스트일 수 있습니까?

호스트가 스푸핑을 시도하지는 않지만 MAC-IP 바인딩 데이터가 DHCP 스누핑 바인딩 데이터베이스에 없기 때문에 네트워크에서 격리됩니다.

고정 호스트는 IP 주소에 정적으로 할당되었으므로 DHCP를 사용하여 IP 주소를 받지 않았기 때문입니다.

고정 IP 주소가 있는 정상 호스트에 연결을 제공하기 위해 구현할 수 있는 몇 가지 해결 방법이 있습니다.

옵션 1.

ip arp 검사 트러스트를 사용하여 호스트에 연결된 인터페이스를 구성합니다.

```
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
```

옵션 2.

ARP Access-List를 사용하여 고정 호스트를 허용합니다.

```
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
```

옵션 3.

고정 호스트에 대한 바인딩 테이블 항목을 구성합니다.

```
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

DAI에서 사용할 수 있는 추가 옵션:

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

src-mac의 경우 이더넷 헤더의 소스 MAC 주소를 ARP 본문의 발신자 MAC 주소와 비교하여 확인합니다. 이 확인은 ARP 요청 및 응답에 대해 모두 수행됩니다. 활성화하면 서로 다른 MAC 주소를 가진 패킷은 유효하지 않은 것으로 분류되어 삭제됩니다

dst-mac의 경우 이더넷 헤더의 대상 MAC 주소를 ARP 본문의 대상 MAC 주소와 비교하여 확인합니다. 이 확인은 ARP 응답에 대해 수행됩니다. 활성화하면 서로 다른 MAC 주소를 가진 패킷은 유효하지 않은 것으로 분류되고 삭제됩니다.

IP의 경우 ARP 본문에서 유효하지 않거나 예기치 않은 IP 주소를 확인합니다. 주소에는 0.0.0.0, 255.255.255.255 및 모든 IP 멀티캐스트 주소가 포함됩니다. 발신자 IP 주소는 모든 ARP 요청 및 응답에서 확인되며 대상 IP 주소는 ARP 응답에서만 확인됩니다.

ARP 속도 제한을 구성할 수도 있습니다. 기본적으로 신뢰할 수 없는 인터페이스의 ARP 트래픽에는 15pps 제한이 있습니다.

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

IP Source Guard

- IPSG는 DHCP 스누핑 바인딩 데이터베이스 및 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하여 라우팅되지 않은 레이어 2 인터페이스의 IP 트래픽을 제한하는 보안 기능입니다.

- 호스트가 인접 디바이스의 IP 주소를 사용하려고 할 경우 IPSG를 사용하여 트래픽 공격을 방지할 수 있습니다.

- 신뢰할 수 없는 인터페이스에서 DHCP 스누핑이 활성화된 경우 IPSG를 활성화할 수 있습니다. 인터페이스에서 IPSG가 활성화되면 스위치는 DHCP 스누핑에서 허용하는 DHCP 패킷을 제외하고 인터페이스에서 수신된 모든 IP 트래픽을 차단합니다.

- 이 스위치는 하드웨어의 소스 IP 조회 테이블을 사용하여 IP 주소를 포트에 바인딩합니다. IP 및 MAC 필터링의 경우 소스 IP 및 소스 MAC 조회의 조합이 사용됩니다. 바인딩 테이블에 소스 IP 주소가 있는 IP 트래픽이 허용되며 다른 모든 트래픽은 거부됩니다.

- IP 소스 바인딩 테이블에는 DHCP 스누핑에 의해 학습되거나 수동으로 구성된 바인딩이 있습니다(정적 IP 소스 바인딩). 이 테이블의 항목에는 IP 주소, 연결된 MAC 주소 및 연결된 VLAN 번호가 있습니다. 스위치는 IP 소스 가드가 활성화된 경우에만 IP 소스 바인딩 테이블을 사용합니다.

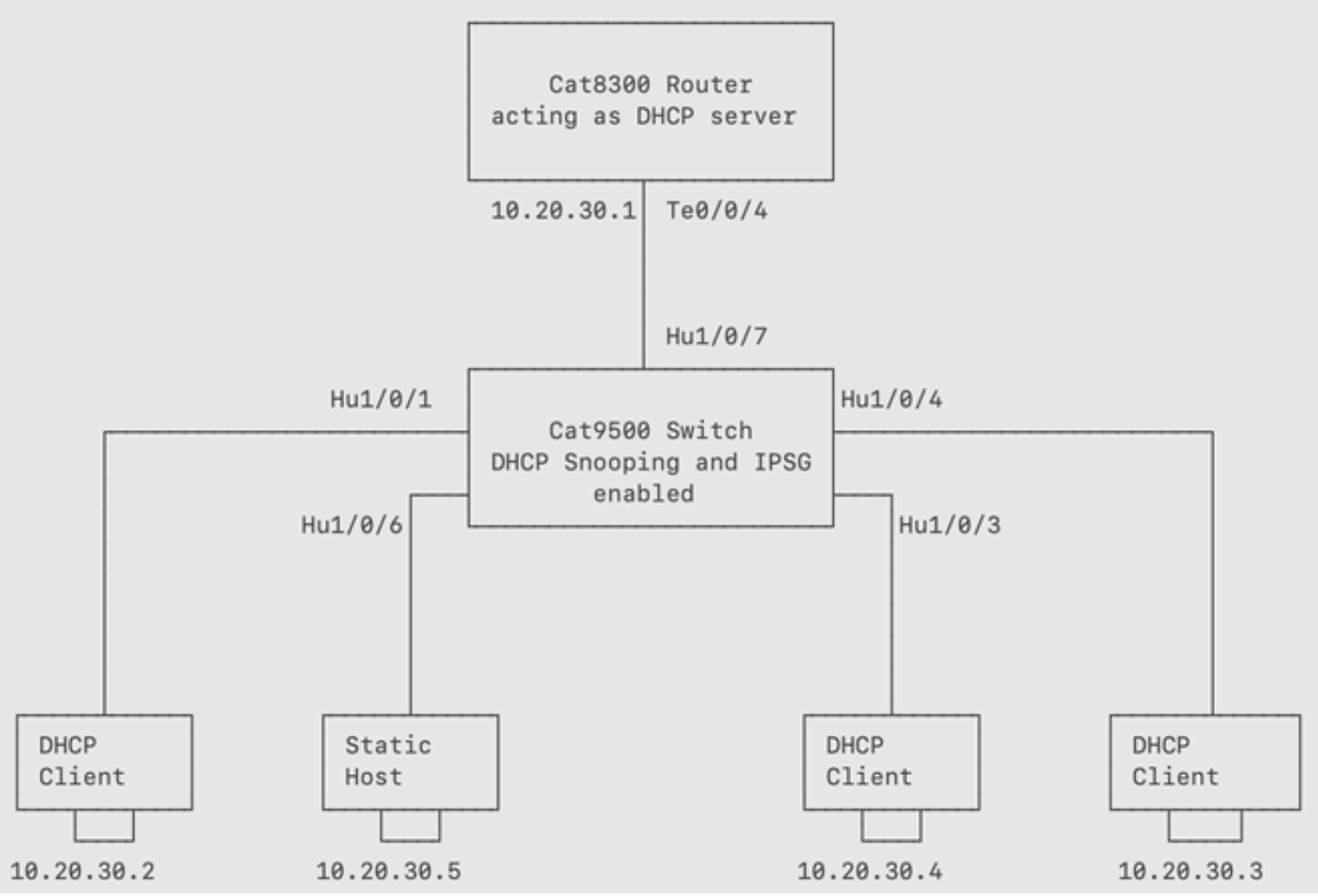
- 소스 IP 주소 필터링 또는 소스 IP 및 MAC 주소 필터링으로 IPSG를 구성할 수 있습니다.

고정 호스트용 IPSG

- 고정 호스트용 IPSG는 IPSG가 DHCP 없이 작동하도록 허용합니다. 고정 호스트용 IPSG는 IP 디바이스 추적 테이블 항목을 사용하여 포트 ACL을 설치합니다. 스위치는 ARP 요청 또는 기타 IP 패킷을 기반으로 고정 엔트리를 생성하여 지정된 포트에 대한 유효한 호스트 목록을 유지합니다.

참조:

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 스위치는 4개의 호스트에 연결되며, 그중 3개의 호스트는 DHCP 클라이언트이고 1개의 호스트는 고정 IP 주소를 갖습니다. DHCP 서버는 DHCP 풀로 구성된 Cat8300 시리즈 라우터입니다.
이 토폴로지를 사용하여 IPSG가 DHCP 스누핑 바인딩 데이터베이스에 없는 MAC-IP 바인딩의 호스트에서 트래픽을 탐지하고 차단하는 방법을 시연할 수 있습니다.

구성:

1단계. Cat9500 스위치에서 DHCP 스누핑을 전역적으로 구성합니다.

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

2단계. DHCP 서버에 연결된 인터페이스 Te1/0/7을 신뢰할 수 있는 포트로 구성합니다. 이렇게 하면 DHCP 오퍼가 인터페이스를 인그레스(ingress)하고 DHCP 클라이언트에 도달할 수 있습니다.

```
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
```

3단계. DHCP 클라이언트에 연결된 포트를 VLAN 10을 허용하는 액세스 포트로 구성합니다.

```
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
```

4단계. DHCP 클라이언트가 DHCP 서버에서 IP 주소를 받았는지 확인합니다.

```
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 TenGigabitEthernet0/0/4

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 TenGigabitEthernet0/0/4

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 TenGigabitEthernet0/0/4

6334.662e.3532.3031.

2e61.6163.632d.5465.

312f.302f.35

5단계. 모든 종단 호스트에 연결된 인터페이스(3x DHCP 클라이언트 및 고정 IP 주소가 있는 1x 호스트)에서 IPSG를 구성합니다.

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
```

확인:

```
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
```

이 출력에서 DHCP 스누핑 바인딩 테이블에 이 인터페이스에 해당하는 MAC-IP 바인딩이 없기 때문에 Hu1/0/6에 대해 IP Address(IP 주소) 필드가 deny-all로 설정된 것을 볼 수 있습니다.

6단계. Static_Host에서 IP 주소 10.20.30.2, 10.20.30.3 및 10.20.30.4로 DHCP 클라이언트를 ping해 봅니다.

```
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 Hu1/0/6
```

```
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
```

IPSG에서 사용할 수 있는 추가 옵션:

기본적으로 IPSG는 IP 주소만을 기준으로 신뢰할 수 없는 포트에서 수신 트래픽을 필터링합니다.
IP 및 MAC 주소를 모두 기반으로 필터링을 수행하려면 다음 단계를 수행합니다.

```
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
```

이 출력에서 Filter-type(필터 유형)이 ip-mac임을 확인할 수 있습니다. 따라서 이제 스위치는 소스 IP 및 MAC 주소를 기반으로 이러한 인터페이스의 수신 패킷을 필터링합니다.

DAI 및 IPSG 문제 해결 팁

- DAI 및 IPSG 관련 문제를 해결할 때 가장 먼저 확인해야 할 사항은 DHCP 스누핑 바인딩 테이블이 올바르게 입력되었는지 확인하는 것입니다.

- 이러한 기능을 활성화하기 전에 고정 IP 주소로 엔드포인트를 처리합니다. 이러한 디바이스의 연결이 끊어지지 않도록 하려면 정적 바인딩을 구성하거나 앞서 언급한 방법 중 하나를 사용하여 스위치에서 이러한 엔드포인트를 신뢰하도록 하십시오.

- DHCP 스누핑이 아직 활성화되지 않았고 클라이언트가 DHCP 서버에서 IP를 이미 수신한 환경에서 DAI 또는 IPSG를 구성하는 동안 먼저 DHCP 스누핑을 활성화하고 다음 두 단계 중 하나를 수행합니다.

  - 클라이언트가 연결된 인터페이스를 반송하여 임대를 갱신합니다.

  - 고객이 자동으로 리스를 갱신할 때까지 기다립니다. 이 경우 시간이 더 걸릴 수 있지만 수동으로 클라이언트에 연결된 모든 포트를 바운스하는 번거로움이 줄어듭니다.

- 위의 두 단계 중 하나를 수행하면 새 DORA 트랜잭션이 트리거됩니다. 스위치에서 DORA 패킷을 스니핑하고 바인딩 테이블을 업데이트합니다. 이 작업을 수행하지 않고 DHCP 스누핑을 구성한 후 DAI 또는 IPSG가 즉시 활성화되면 네트워크의 모든 DHCP 클라이언트가 네트워크에 대한 연결이 끊어지는 문제가 발생할 수 있습니다.

- DAI 또는 IPSG가 구성된 환경에서 연결 문제를 해결하는 동안 DHCP 스누핑 바인딩 테이블이 손상되지 않았는지 확인합니다. 스위치가 이 테이블이 저장된 데이터 구조에 액세스할 수 있는지 확인합니다.

- 바인딩 테이블을 미디어로 내보내면 스위치가 부팅된 후 초기화되는 데 시간이 걸리거나 어떤 이유로 인해 스위치에 액세스할 수 없게 되는 경우가 있을 수 있습니다. 이러한 시나리오에서 연결 문제가 발견되었을 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.