# Probleemoplossing voor Dynamic ARP Inspection (DAI) en IP Source Guard (IPSG) in Catalyst Switches

## Inhoud



## Inleiding

Dit document beschrijft hoe Dynamic ARP Inspection (DAI) en IP Source Guard (IPSG) werken en hoe u deze in Catalyst 9K-Switches kunt valideren.

## DHCP-controle en verwante functies

Alvorens in DAI en IPSG te duiken, moet u kort over DHCP Snooping bespreken, die een eerste vereiste aan DAI en IPSG is.

Dynamic Host Configuration Protocol (DHCP) is een client/serverprotocol dat automatisch een Internet Protocol (IP)-host voorziet van zijn IP-adres en andere bijbehorende configuratieinformatie, zoals het subnetmasker en de standaardgateway. RFC's 2131 en 2132 definiëren DHCP als een Internet Engineering Task Force (IETF) standaard gebaseerd op Bootstrap Protocol (BOOTP), een protocol waarmee DHCP veel implementatiedetails deelt. DHCP biedt hosts de vereiste TCP/IP-configuratieinformatie van een DHCP-server.

DHCP-snuffelen is een beveiligingsfunctie die werkt als een firewall tussen onvertrouwde hosts en vertrouwde DHCP-servers. De DHCP-snuffelfunctie voert deze activiteiten uit:

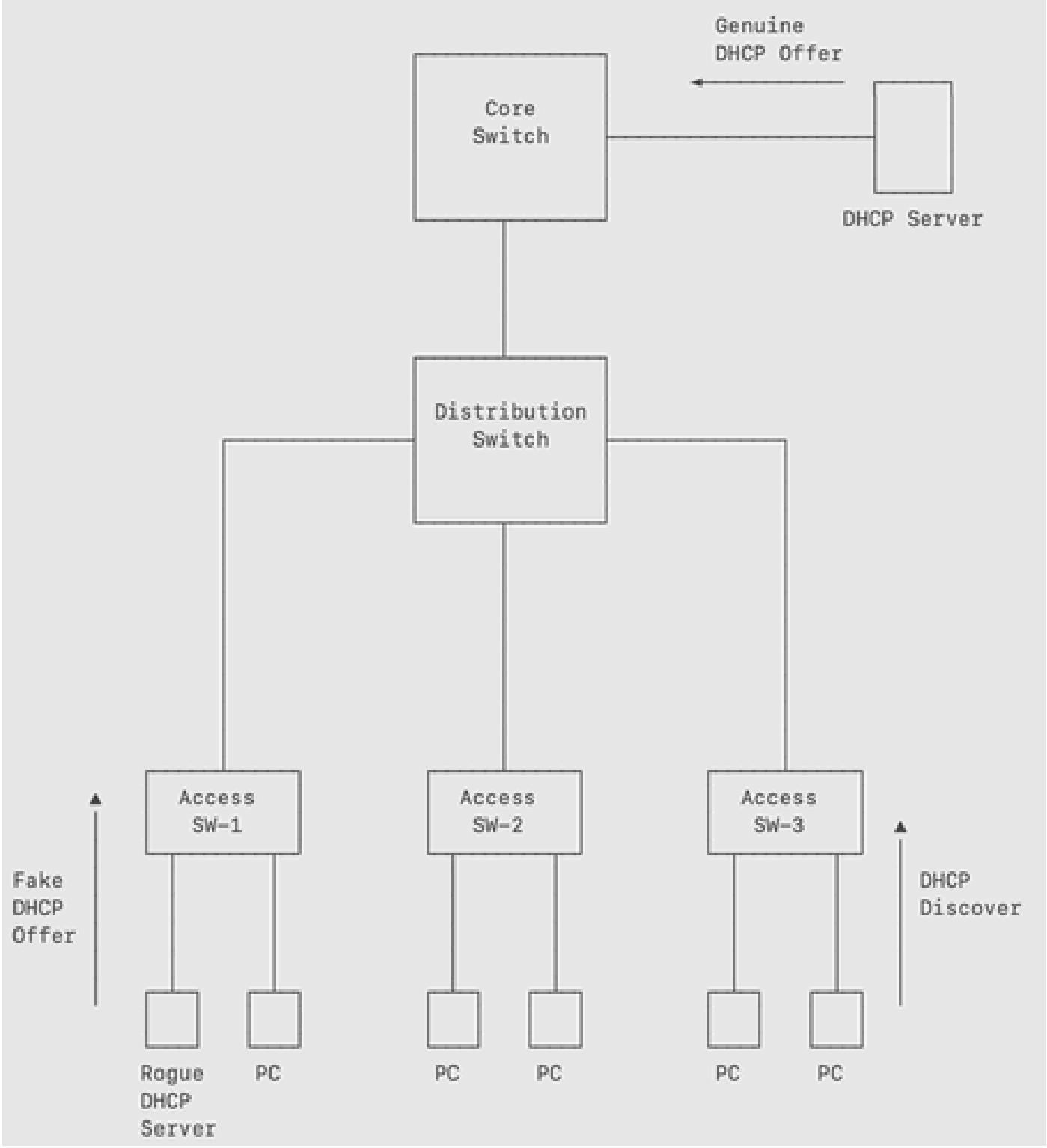
- Bevestigt DHCP-berichten die worden ontvangen van onbetrouwbare bronnen en filtert ongeldige berichten uit.
- Rate-limieten DHCP-verkeer van vertrouwde en onbetrouwbare bronnen.
- Biedt en onderhoudt de DHCP spioping bindende database, die informatie bevat over onvertrouwde hosts met geleasede IP-adressen.

- Gebruikt de DHCP snooping bindende database om latere verzoeken van onbetrouwbare hosts te valideren.

DAI is een beveiligingsfunctie die ARP-pakketten (Address Resolution Protocol) in een netwerk valideert. DAI staat een netwerkbeheerder toe om ARP-pakketten met ongeldige MAC-adressen te onderscheppen, te registreren en te verwerpen aan IP-adresbanden. Deze mogelijkheid beschermt het netwerk tegen bepaalde "man-in-the-middle" aanvallen.

IPSG is een beveiligingsfunctie die IP-verkeer op niet-routed interfaces, Layer 2-interfaces beperkt door verkeer te filteren op basis van de DHCP-snelkieuwelbindingsdatabase en op handmatig geconfigureerde IP-bronbindingen. U kunt IPSG gebruiken om verkeersaanvallen te voorkomen als een host probeert het IP-adres van zijn buur te gebruiken.

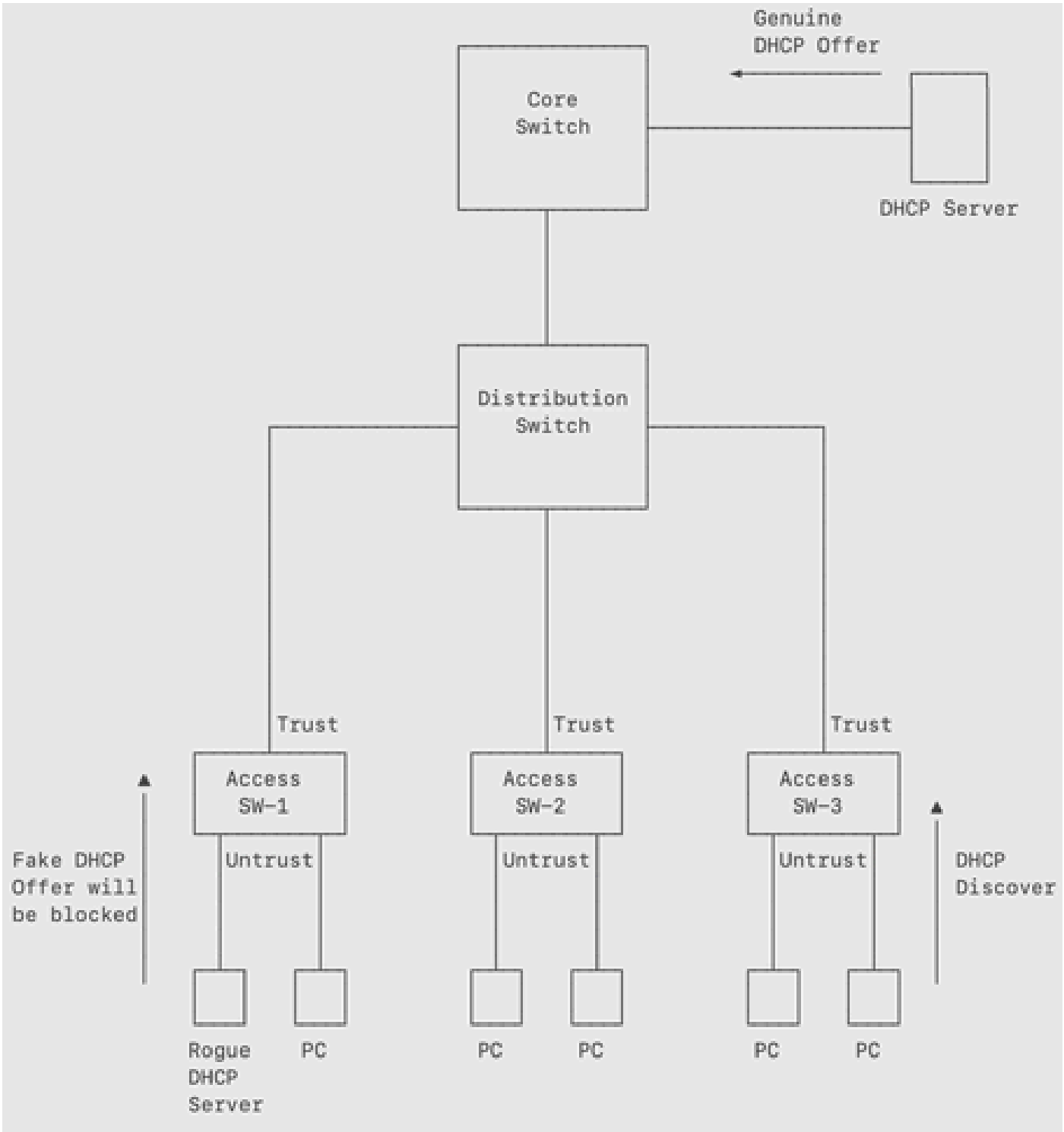
## Scenario zonder DHCP-controle




1. In dit diagram kunt u zien dat meerdere clients een IP-adres willen ontvangen van de DHCP-server die is aangesloten op de Core Switch.
2. Er is echter een kwaadaardige/schurkenDHCP-server die is verbonden met een van de switches op de toegangslaag die de DHCP kan ontvangen en DHCP-aanbiedingen sneller kan verzenden dan de eigenlijke DHCP-server.
3. De aanvaller kan het gatewayadres in het aanbiedingsbericht zo instellen dat hij al het verkeer van de klant kan ontvangen, waardoor de vertrouwelijkheid van de communicatie in het gedrang komt.

4. Dit staat bekend als de man in het midden aanval.

## Scenario met DHCP-controle

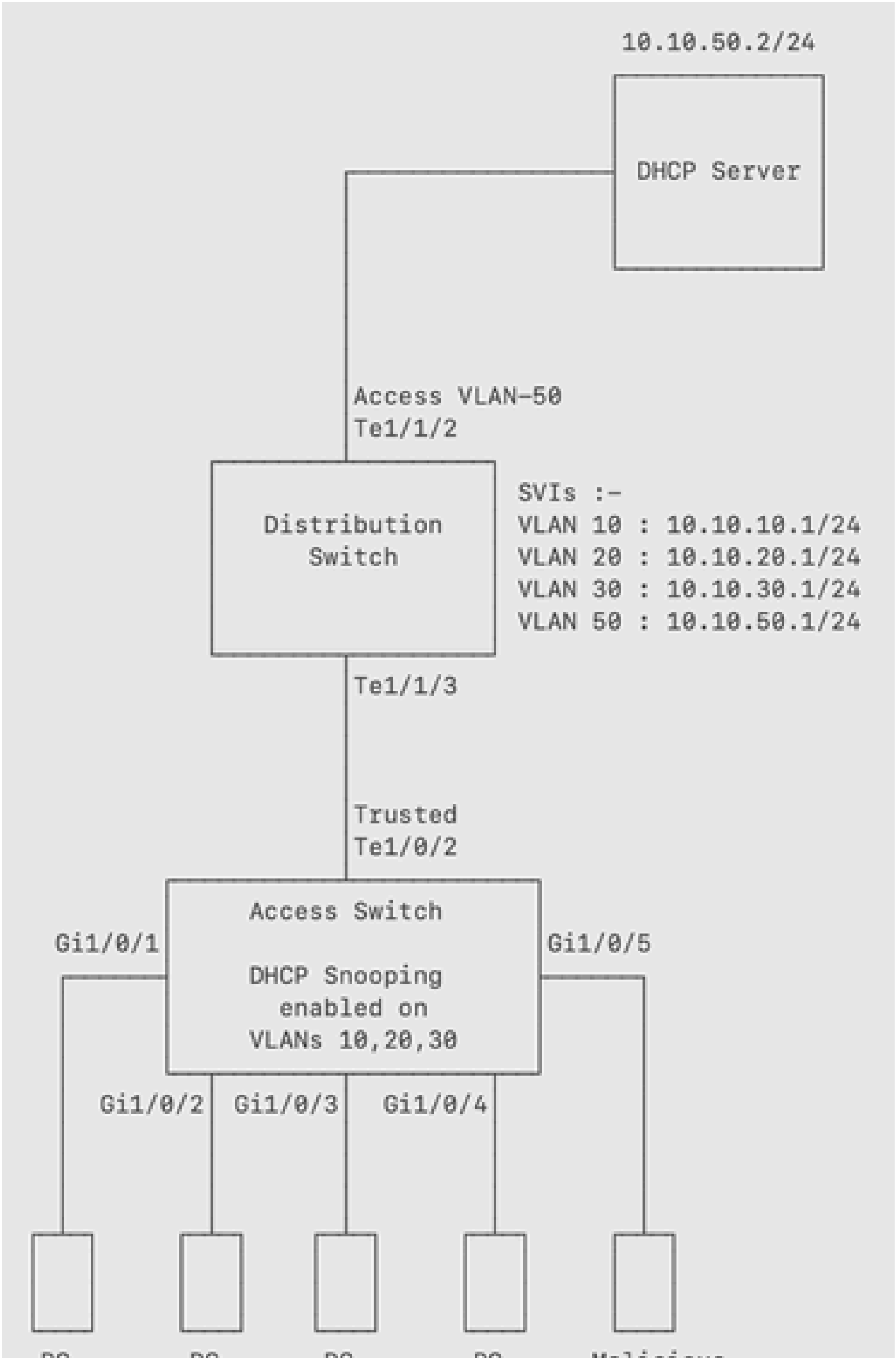



1. Door DHCP-snuffelen in de Access Switches in te schakelen, configureer de switch om te luisteren naar DHCP-verkeer en stop eventuele kwaadaardige DHCP-pakketten die worden ontvangen op onbetrouwbare poorten.
2. Zodra u DHCP-spionage in de Switch inschakelt, worden alle interfaces automatisch onbetrouwbaar.
3. Houd de poorten verbonden met eindapparaten onbetrouwbaar en configureer de poorten die

zijn aangesloten op de echte DHCP-server als vertrouwd.
4. Een onbetrouwbare interface blokkeert DHCP-aanbodberichten. DHCP-aanbiedingsberichten worden alleen toegestaan op vertrouwde poorten.
5. U kunt het aantal DHCP-detectiepakketten beperken die eindhosts per seconde naar een onbetrouwbare interface kunnen verzenden. Dit is een beveiligingsmechanisme om de DHCP-server te beveiligen tegen een abnormaal hoog aantal inkomende DHCP-ontdekkingen die de pool in een mum van tijd kunnen uitputten.

In deze sectie wordt uitgelegd hoe u DHCP-controle in een switched netwerk kunt configureren:

Topologie:


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
```

Stap 2. Configureer het DHCP-snuffelvertrouwen op alle interfaces van de Access Switch die DHCP-aanbiedingen ontvangen van echte DHCP-server(s). Het aantal dergelijke interfaces hangt af van het netwerkontwerp en de plaatsing van DHCP-servers. Dit zijn de interfaces die naar de echte DHCP-server gaan.

Access Switch:

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

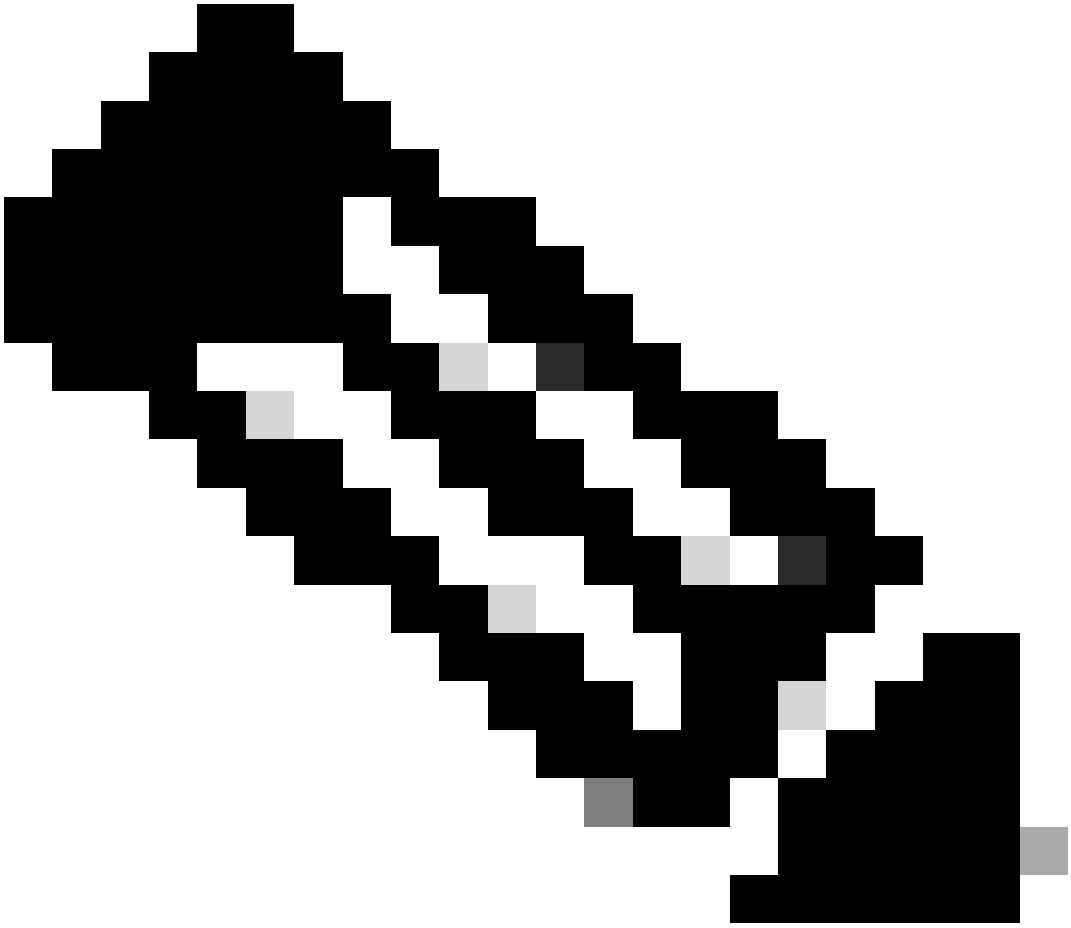
Stap 3. Zodra u DHCP-spionage wereldwijd configureert, worden alle poorten in de Switch automatisch onbetrouwbaar (behalve de poorten die u handmatig vertrouwt, zoals eerder getoond). U kunt echter het aantal DHCP-detectiepakketten configureren die eindhosts per seconde naar onbetrouwbare interfaces kunnen verzenden.
Dit is een beveiligingsmechanisme om de DHCP-server te beveiligen tegen een abnormaal hoog aantal inkomende DHCP-ontdekkingen die de pool in een mum van tijd kunnen uitputten.

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

Verificatie:

```
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:
```



Opmerking: Als u naar deze uitvoer kijkt, ziet u dat Gi1/0/5, die is verbonden met de schadelijke DHCP-server, in de **show ip dhcp snooping** uitvoer wordt vermeld als onbetrouwbaar.

DHCP Snooping doet dus al zijn controles op deze poorten.

Dit zorgt er bijvoorbeeld voor dat alle inkomende DHCP-aanbiedingen op deze poort (Gi1/0/5) worden verwijderd.

Hier is de bindende tabel van DHCP-controle, die het IP-adres, het MAC-adres en de interface voor 3 clients op Gi1/0/1, Gi1/0/2, Gi1/0/3 toont:

```
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
```

Voor demonstratiedoeleinden ip dhcp snooping trust wordt configuratie verwijderd onder Te1/0/2 in de Access Switch. Bekijk de logbestanden die in de Switch worden gegenereerd:

```
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
```

- Zoals u kunt zien, laat de Access Switch inkomende DHCP-aanbodpakketten vallen op Te1/0/2 omdat deze niet langer vertrouwd zijn.

- De MAC-adressen in de logboeken behoren tot de SVI's van VLAN 10,20 en 30 omdat zij degenen zijn die deze aanbiedingen van de DHCP-server naar deze clients verzenden.

**ARP-vergiftiging**

ARP verstrekt IP communicatie binnen een Layer 2 uitzendingsdomein door een IP-adres aan een MAC-adres in kaart te brengen. Het is een eenvoudig protocol, maar kwetsbaar voor aanvallen die ARP-vergiftiging worden genoemd.

ARP-vergiftiging is een aanval waarbij een aanvaller een nep ARP-antwoordpakketten naar het netwerk stuurt.

Een kwaadaardige gebruiker kan hosts, switches en routers aanvallen die zijn aangesloten op uw Layer 2-netwerk door de ARP-caches te vergiftigen van systemen die zijn aangesloten op het subnetnetwerk en door verkeer dat is bedoeld voor andere hosts op het subnetnetwerk te onderscheppen

Dit is de klassieke Man-in-the-middle aanval.

Preventiemechanismen

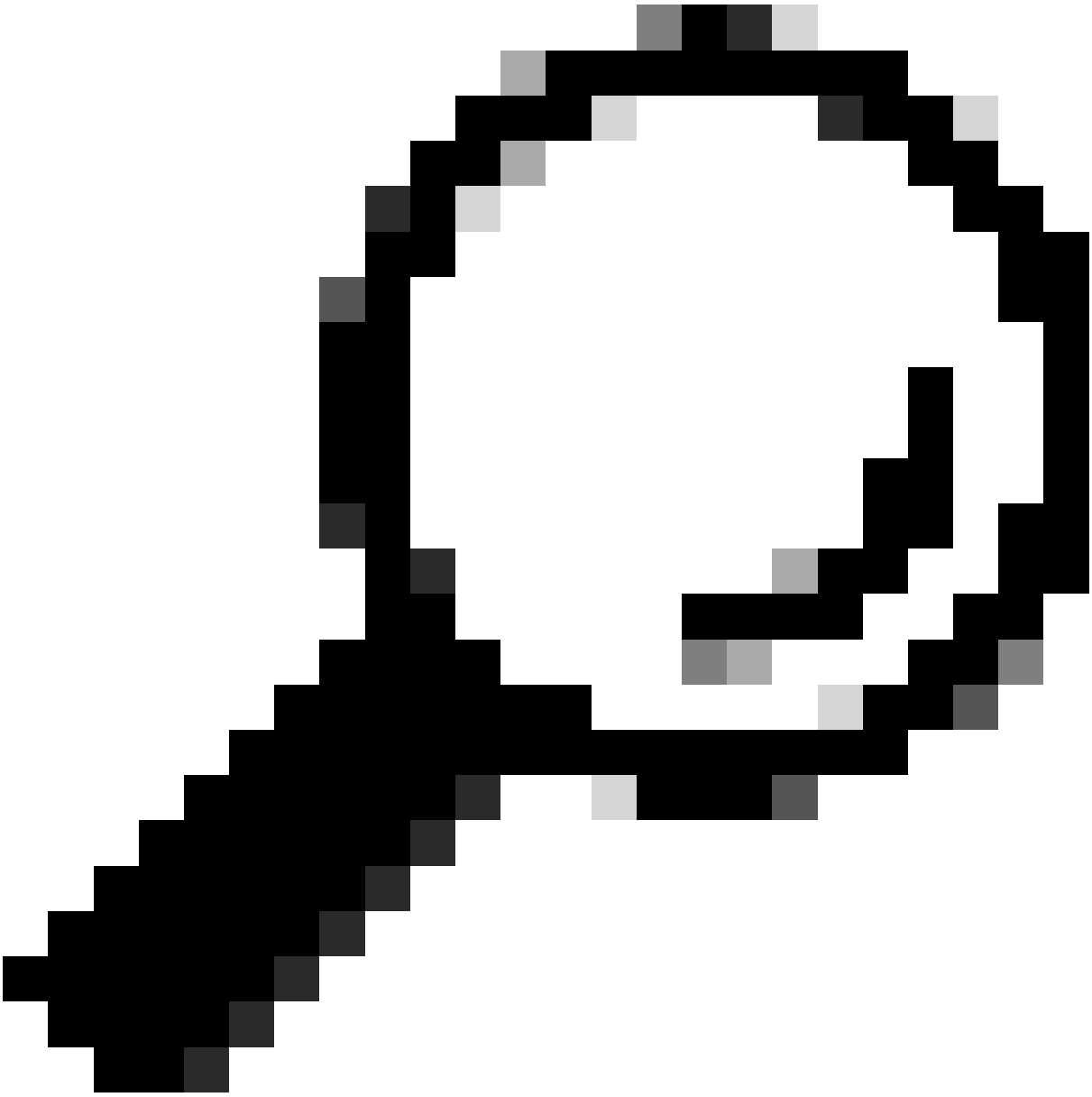
Dynamische ARP-inspectie (DAI)

Dynamische ARP-inspectie is een beveiligingsfunctie die ARP-pakketten in een netwerk valideert. Het onderschept, logt, en verwerpt ARP pakketten met ongeldige IP-aan-MAC adresbanden in. Deze mogelijkheid beschermt het netwerk tegen bepaalde man-in-the-middle aanvallen.

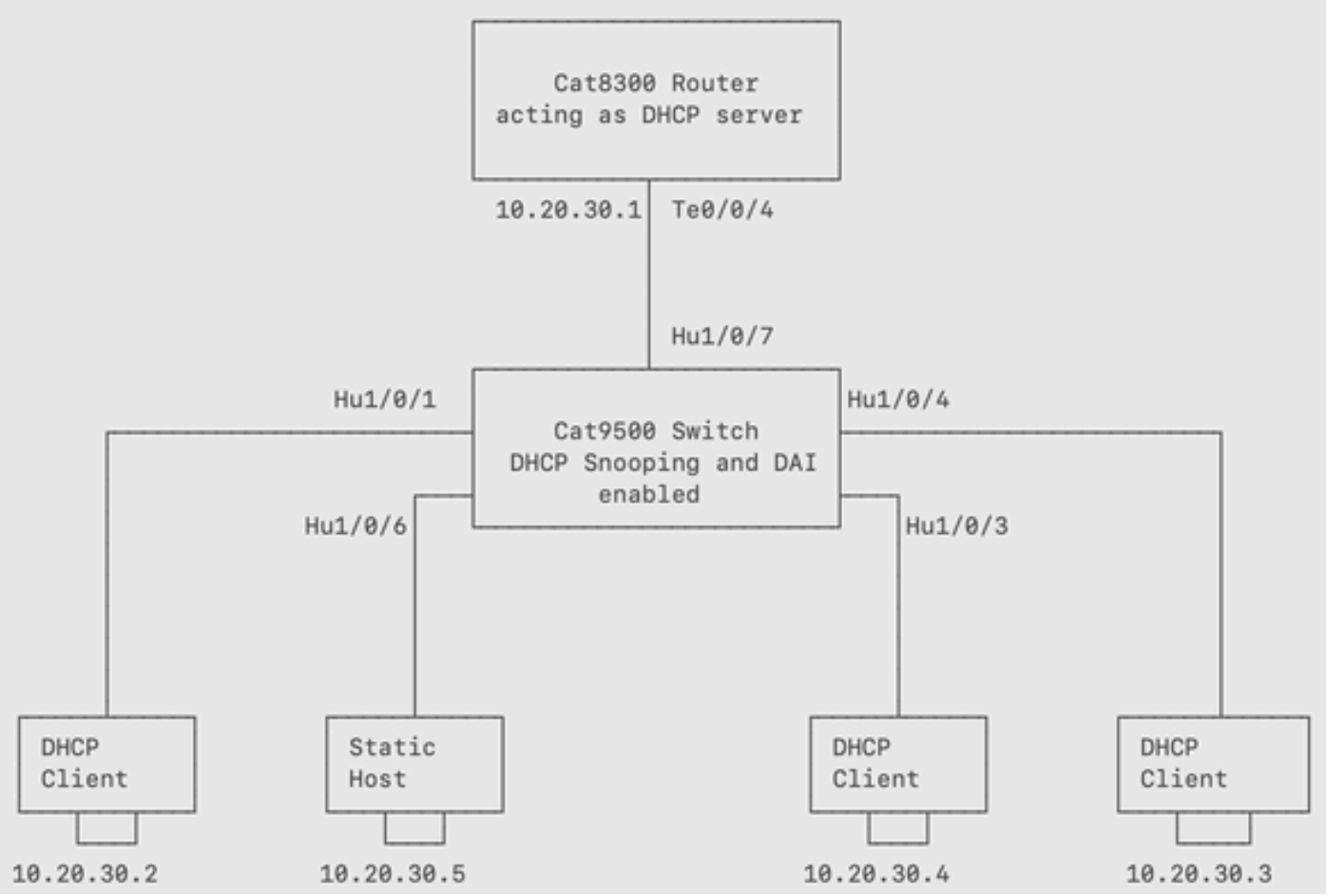
Dynamische ARP-inspectie zorgt ervoor dat alleen geldige ARP-verzoeken en antwoorden worden doorgestuurd. De switch voert de volgende activiteiten uit:

- onderschept alle ARP verzoeken en antwoorden op onbetrouwbare poorten
- Verifieert dat elk van deze onderschepte pakketten een geldige IP-naar-MAC-adresband heeft voordat de lokale ARP-cache wordt bijgewerkt of voordat het pakket naar de juiste bestemming wordt doorgestuurd
- Dropt ongeldige ARP-pakketten

Dynamische ARP-inspectie bepaalt de geldigheid van een ARP-pakket op basis van geldige IP-naar-MAC-adresbindingen die zijn opgeslagen in een vertrouwde database, de DHCP-snooping binddatabase.
Dit gegevensbestand wordt gebouwd door het snooping van DHCP als het snooping van DHCP op VLANs en op de switch wordt toegelaten.
Als het ARP-pakket op een vertrouwde interface wordt ontvangen, stuurt de switch het pakket zonder enige controles door.
Voor onbetrouwbare interfaces, door:sturen de switch het pakket slechts als het geldig is.



**Tip**: raadpleeg 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




Deze afbeelding toont Cat9500 Switch aangesloten op vier hosts, waarvan 3 hosts DHCP-clients zijn en 1 host een statisch IP-adres heeft (10.20.30.5). De DHCP-server is een Cat8300 Series router geconfigureerd met een DHCP-pool.

De bovenstaande topologie wordt gebruikt om aan te tonen hoe DAI ongeldige ARP-verzoeken detecteert op een interface en het netwerk beschermt tegen kwaadaardige aanvallers.

Configuratie:

Stap 1. DHCP-snuffelen en DAI wereldwijd configureren in de 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
```

Stap 2. Configureer de interface Hu1/0/7 die is verbonden met de DHCP-server als een vertrouwde poort. Dit zal de aanbiedingen van DHCP toestaan om de interface in te gaan en later de cliënten van DHCP te bereiken.

```
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
```

Stap 3. Configureer de poorten die met de DHCP-clients zijn verbonden als toegangspoorten die VLAN 10 toestaan.

```
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
```

Stap 4. Controleer of de DHCP-clients IP-adres hebben ontvangen van de DHCP-server, van de DHCP Snooping bindtabel in de 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
```

U kunt de banden in de DHCP-server ook controleren.

```
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

Stap 5: Verander het IP-adres van de host die is aangesloten op Hu1/0/6 van 10.20.30.5 naar 10.20.30.2 en probeer de andere DHCP-clients van die host te pingen.

```
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:
.....
```

Deze ongeldige ARP-logbestanden zijn te zien op de 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.([7035.0956.7ee4/10.20.30.2/0000.0000.0000
*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
```

- Zoals u kunt zien, wanneer u probeert om 10.20.30.3 en 10.20.30.4 te pingen van de Static_Host, kunt u dit niet doen. Alhoewel Static_Host het IP-adres van de legale DHCP-client probeerde te paren, was dit niet mogelijk omdat elk ARP-pakket dat op Hu1/0/6 aankomt, door de Switch zal worden geïnspecteerd en vergeleken met de gegevens in de DHCP-snooping-bindingstabel.

- De daaropvolgende logboeken van de Cat9500 Switch bevestigen dat de ARP-verzoeken die van de Static_Host naar de DHCP-clients worden verzonden, worden gedropt.

- De Cat9500 Switch bereikt dit door het verwijzen van de DHCP snooping binddatabase.

- Wanneer een ARP verzoek Hu1/0/6 met de bron MAC-IP ingaat die niet de waarden huidig in het het snooping bindende gegevensbestand van DHCP aanpast, zal de Switch het ARP verzoek laten vallen.

Stap 6. Verificatie:

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 |

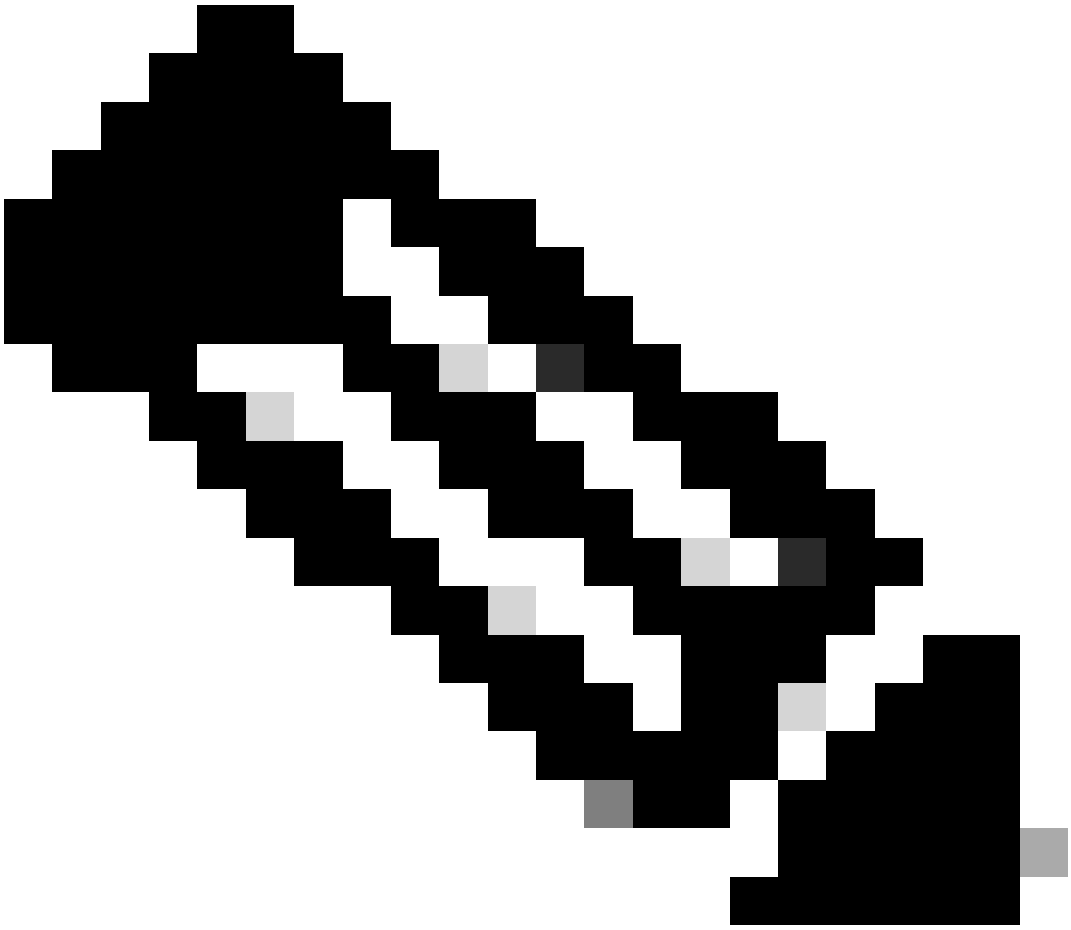
| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|---|---|---|---|---|
| 10 | 9 | 39 | 39 | 0 |

| 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 deze uitvoer, kunt u het aantal pakketten zien die door DAI in VLAN 10 in de Switch Cat9500 worden gelaten vallen en toegestaan.

---



**Opmerking**: Een zeer belangrijk scenario kan een legitieme host in het netwerk zijn die een Statisch IP-adres (bijv. 10.20.30.5) heeft toegewezen?

Alhoewel de host niets probeert te parodiëren, zal het nog steeds geïsoleerd worden van het netwerk omdat zijn MAC-IP bindende gegevens niet aanwezig zijn in de DHCP snooping bindende database.

Dit komt doordat de statische host nooit DHCP heeft gebruikt om het IP-adres te ontvangen, omdat het statisch aan het adres is toegewezen.

---

We hebben een paar workarounds die kunnen worden geïmplementeerd om connectiviteit te bieden aan legale hosts die statische IP-adressen hebben.

---

Optie 1.

Configureer de interface die is aangesloten op de host met de 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
```

Optie 2.

Sta de statische host toe met behulp van een ARP-toegangslijst:

```
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

Optie 3.

Configureer een bindende tabelingang voor de statische 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
```

Extra opties beschikbaar bij 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
```

Voor src-mac, controleer het adres bron van MAC in de kopbal Ethernet tegen het adres van afzenderMAC in het ARP lichaam. Deze controle wordt uitgevoerd op zowel ARP verzoeken als reacties. Als deze optie is ingeschakeld, worden pakketten met verschillende MAC-adressen als ongeldig geclassificeerd en worden deze gedropt

Voor dst-mac, controleer het adres van bestemmingsMAC in de kopbal Ethernet tegen het adres van doelMAC in ARP lichaam. Deze controle wordt uitgevoerd voor ARP reacties. Als deze optie is ingeschakeld, worden pakketten met verschillende MAC-adressen geclassificeerd als ongeldig en worden deze verwijderd.

Controleer voor IP de ARP-body op ongeldige en onverwachte IP-adressen. Adressen omvatten 0.0.0.0, 255.255.255.255 en alle IP-multicast adressen. IP-adressen van afzenders worden gecontroleerd in alle ARP-verzoeken en antwoorden, en IP-adressen van doelapparaten worden alleen gecontroleerd in ARP-antwoorden.

U kunt ook ARP snelheidsbeperking configureren. Standaard is er een limiet van 15 pps voor ARP-verkeer op onbetrouwbare interfaces:

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

IP-bronbewaker

- IPSG is een beveiligingsfunctie die IP-verkeer op niet-gerouteerde, Layer 2-interfaces beperkt door verkeer te filteren op basis van de DHCP-snelkieuwelbindingsdatabase en handmatig geconfigureerde IP-bronbanden.

- U kunt IPSG gebruiken om verkeersaanvallen te voorkomen als een host probeert het IP-adres van zijn buur te gebruiken.

- U kunt IPSG inschakelen wanneer DHCP-snooping is ingeschakeld op een onbetrouwbare interface. Nadat IPSG is ingeschakeld op een interface blokkeert de switch al het IP-verkeer dat op de interface wordt ontvangen, behalve voor DHCP-pakketten die zijn toegestaan door DHCP-snooping.

- De switch gebruikt een IP-zoektabel in de hardware om IP-adressen aan poorten te binden. Voor IP- en MAC-filtering wordt een combinatie van IP-bron en MAC-bron gebruikt. IP-verkeer met een IP-bronadres in de bindende tabel is toegestaan, wordt al het andere verkeer geweigerd.

- De IP-bronbindingstabel heeft bindingen die door DHCP-snuffelen worden geleerd of handmatig worden ingesteld (statische IP-bronbindingen). Een ingang in deze tabel heeft een IP-adres, het bijbehorende MAC-adres en het bijbehorende VLAN-nummer. De switch gebruikt de bindende tabel voor IP-bronnen alleen wanneer de IP-bronbeveiliging is ingeschakeld.

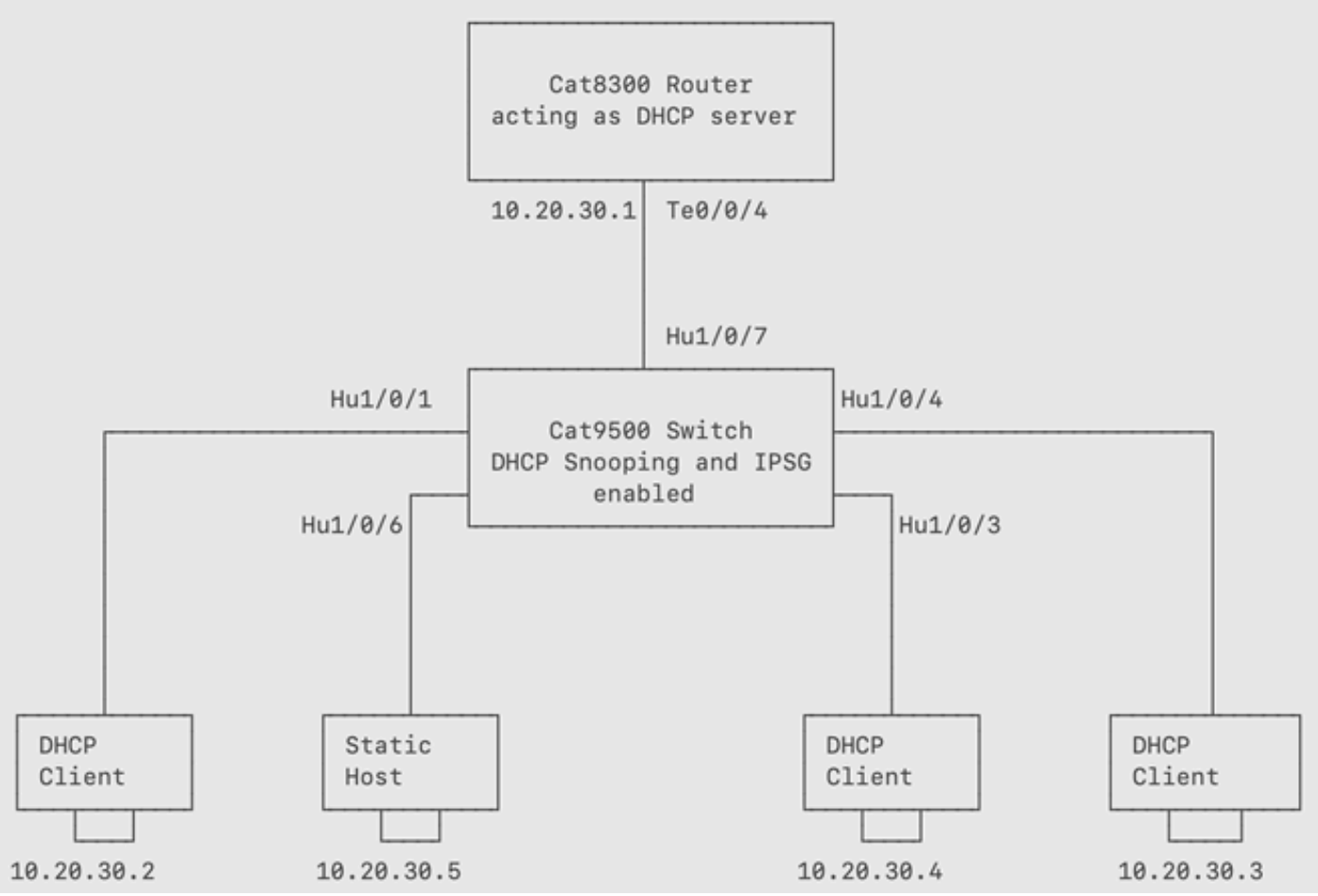
- U kunt IPSG configureren met bronIP-adresfiltering of met bronIP- en MAC-adresfiltering.

IPSG voor statische hosts

- IPSG voor statische hosts maakt het mogelijk dat IPSG zonder DHCP werkt. IPSG voor statische hosts maakt gebruik van de vermeldingen in de traceertabel van IP-apparaten om poortACL's te installeren. De switch maakt statische vermeldingen op basis van ARP-verzoeken of andere IP-pakketten om de lijst met geldige hosts voor een bepaalde poort te handhaven.

Referentie:

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 verbonden met vier hosts waarvan 3 hosts DHCP-clients zijn en 1 host een statisch IP-adres heeft. De DHCP-server is een Cat8300 Series router geconfigureerd met een DHCP-pool.
U kunt deze topologie gebruiken om aan te tonen hoe IPSG verkeer detecteert en blokkeert van hosts waarvan MAC-IP-bindingen niet aanwezig zijn in de DHCP-snooping-bindingsdatabase.

Configureren:

Stap 1. DHCP-spionage wereldwijd configureren in de 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

Stap 2. Configureer de interface Te1/0/7 die is verbonden met de DHCP-server als een vertrouwde poort. Dit staat de aanbiedingen van DHCP toe om de interface in te gaan en later de cliënten van DHCP te bereiken.

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
```

Stap 3. Configureer de poorten die met de DHCP-clients zijn verbonden als toegangspoorten die VLAN 10 toestaan.

```
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
```

Stap 4. Controleer of de DHCP-clients het IP-adres van de DHCP-server hebben ontvangen.

```
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

Stap 5. Configureer IPSG onder de interfaces die zijn aangesloten op alle eindhosts (3x DHCP-clients en 1x host met statisch IP-adres).

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
```

Verificatie:

```
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
```

Van deze output, kunt u zien het IP veld Adres is ingesteld op deny-all voor Hu1/0/6 omdat er geen MAC-IP-band is die overeenkomt met deze interface in de DHCP snooping bindende tabel.

Stap 6. Probeer de DHCP-clients met IP-adressen 10.20.30.2, 10.20.30.3 en 10.20.30.4 van de Static_Host te pingen.

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
```

Aanvullende opties beschikbaar met IPSG:

Standaard filtert IPSG inkomend verkeer op onbetrouwbare poorten die alleen op IP-adressen zijn gebaseerd.

Als u het filteren wilt uitvoeren op basis van zowel IP- als MAC-adres, voert u deze stappen uit.

```
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 deze uitvoer kunt u zien dat het filtertype ip-mac is. De Switch filtert nu de inkomende pakketten op deze interfaces op basis van zowel IP-bron als MAC-adres.

#### Tips voor probleemoplossing voor DAI en IPSG

- Het eerste te controleren ding terwijl het oplossen van problemen DAI en IPSG-gerelateerde problemen is te verifiëren als de DHCP snooping bindende tabel correct is bevolkt.

- Alvorens deze functies in te schakelen, dient u de eindpunten te behandelen met statische IP-adressen. Als u niet wilt dat deze apparaten bereikbaar verliezen, configureer dan statische bindingen of gebruik een van de eerder genoemde methodologieën om de Switch deze endpoints te vertrouwen.

- Tijdens het configureren van DAI of IPSG in een omgeving waarin DHCP-snuffelen nog niet is ingeschakeld en clients al IP's hebben ontvangen van de DHCP-server, moet u eerst DHCP-snuffelen inschakelen en een van de twee stappen uitvoeren:

    - Bounce de client-verbonden interfaces zodat zij hun lease verlengen.

    - Wacht tot de klanten hun leaseovereenkomst automatisch verlengen. Dit kan meer tijd in beslag nemen, maar bespaart u het gemak van het handmatig weerkaatsen van alle op de client aangesloten poorten.

- Als een van de twee bovenstaande stappen wordt uitgevoerd, wordt er een nieuwe DORA-transactie gestart. De Switch zal de DORA-pakketten bekijken en de bindende tabel bijwerken. Als dit niet gebeurt en DAI of IPSG onmiddellijk wordt ingeschakeld na het configureren van DHCP-snuffelen, kunt u in een probleem terecht komen waar alle DHCP-clients in het netwerk verbinding met het netwerk verliezen.

- Terwijl het oplossen van problemen connectiviteitskwesties in een milieu waar DAI of IPSG wordt gevormd, zorg ervoor dat de het snooping van DHCP bindende lijst niet wordt bedorven. Zorg ervoor dat de Switch toegang heeft tot de gegevensstructuur waarin deze tabel is opgeslagen.

- Er kunnen gevallen zijn waarin de bindingstabel wordt geëxporteerd naar een medium dat tijd nodig heeft om te worden geïnitialiseerd nadat de switch opstart of ontoegankelijk wordt voor de switch om een of andere reden. Je zou connectiviteitsproblemen kunnen hebben opgemerkt in dergelijke scenario's.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.