Dépannage de l'inspection ARP dynamique (DAI) et de la protection de source IP (IPSG) dans les commutateurs Catalyst

Table des matières

Introduction

Ce document décrit le fonctionnement de Dynamic ARP Inspection (DAI) et IP Source Guard (IPSG), et comment les valider dans les commutateurs Catalyst 9K.

Surveillance DHCP et fonctionnalités associées

Avant de vous plonger dans DAI et IPSG, vous devez aborder brièvement la surveillance DHCP, qui est un prérequis pour DAI et IPSG.

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur qui fournit automatiquement à un hôte IP (Internet Protocol) son adresse IP et d'autres informations de configuration associées, telles que le masque de sous-réseau et la passerelle par défaut. Les documents RFC 2131 et 2132 définissent DHCP comme une norme IETF (Internet Engineering Task Force) basée sur le protocole BOOTP (Bootstrap Protocol), un protocole avec lequel DHCP partage de nombreux détails d'implémentation. Le protocole DHCP permet aux hôtes d’obtenir les informations de configuration TCP/IP requises auprès d’un serveur DHCP.

La surveillance DHCP est une fonctionnalité de sécurité qui agit comme un pare-feu entre des hôtes non approuvés et des serveurs DHCP approuvés. La fonction de surveillance DHCP effectue les activités suivantes :

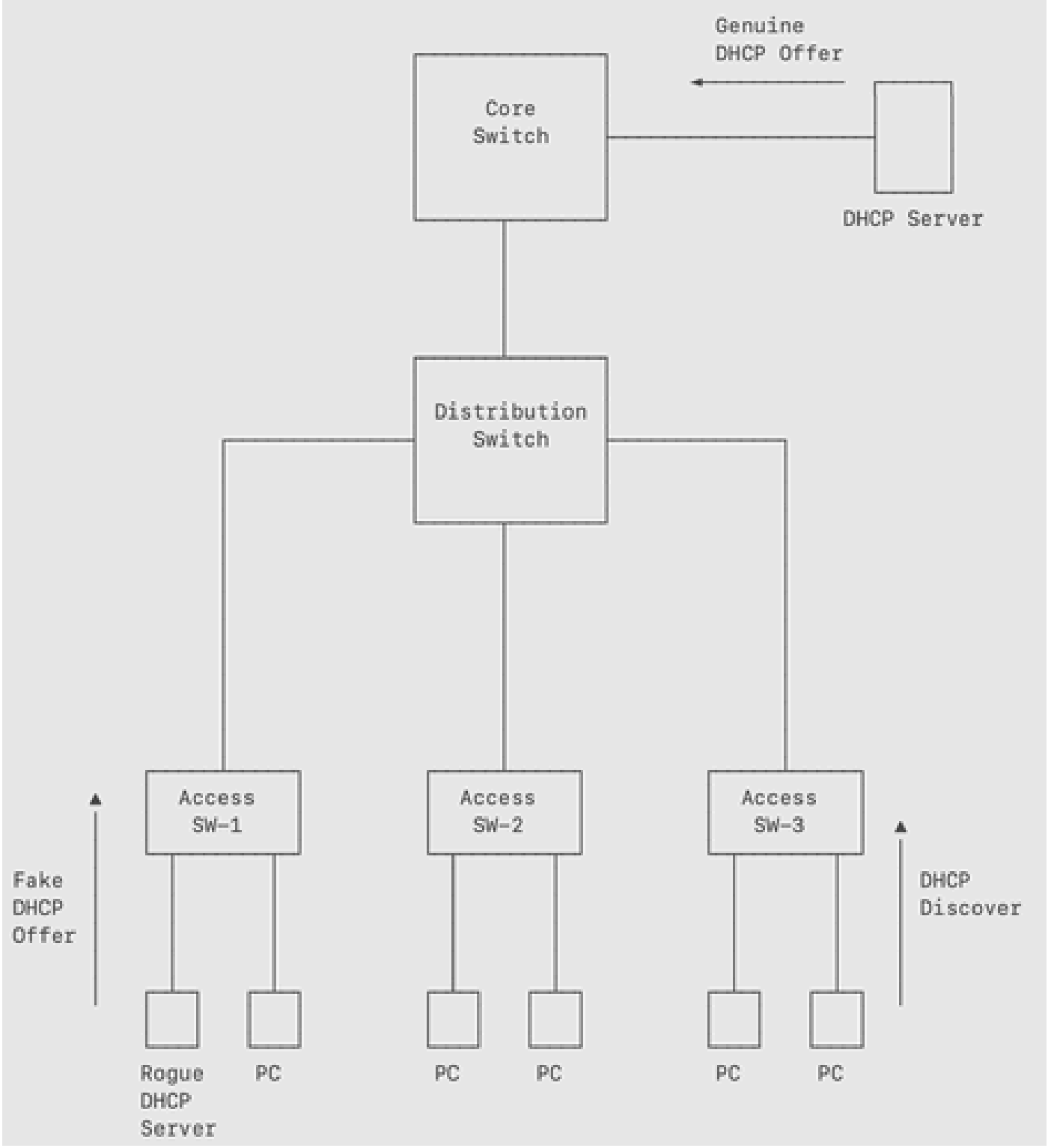
- Valide les messages DHCP reçus de sources non approuvées et filtre les messages non valides.
- Débit : limite le trafic DHCP provenant de sources fiables et non fiables.

- Génère et gère la base de données de liaison de surveillance DHCP, qui contient des informations sur les hôtes non approuvés avec des adresses IP louées.
- Utilise la base de données de liaison de surveillance DHCP pour valider les requêtes suivantes provenant d'hôtes non approuvés.

DAI est une fonction de sécurité qui valide les paquets ARP (Address Resolution Protocol) dans un réseau. L'interface DAI permet à un administrateur réseau d'intercepter, de consigner et d'éliminer les paquets ARP avec des adresses MAC non valides dans les liaisons d'adresses IP. Cette fonctionnalité protège le réseau contre certaines attaques de type « homme du milieu ».

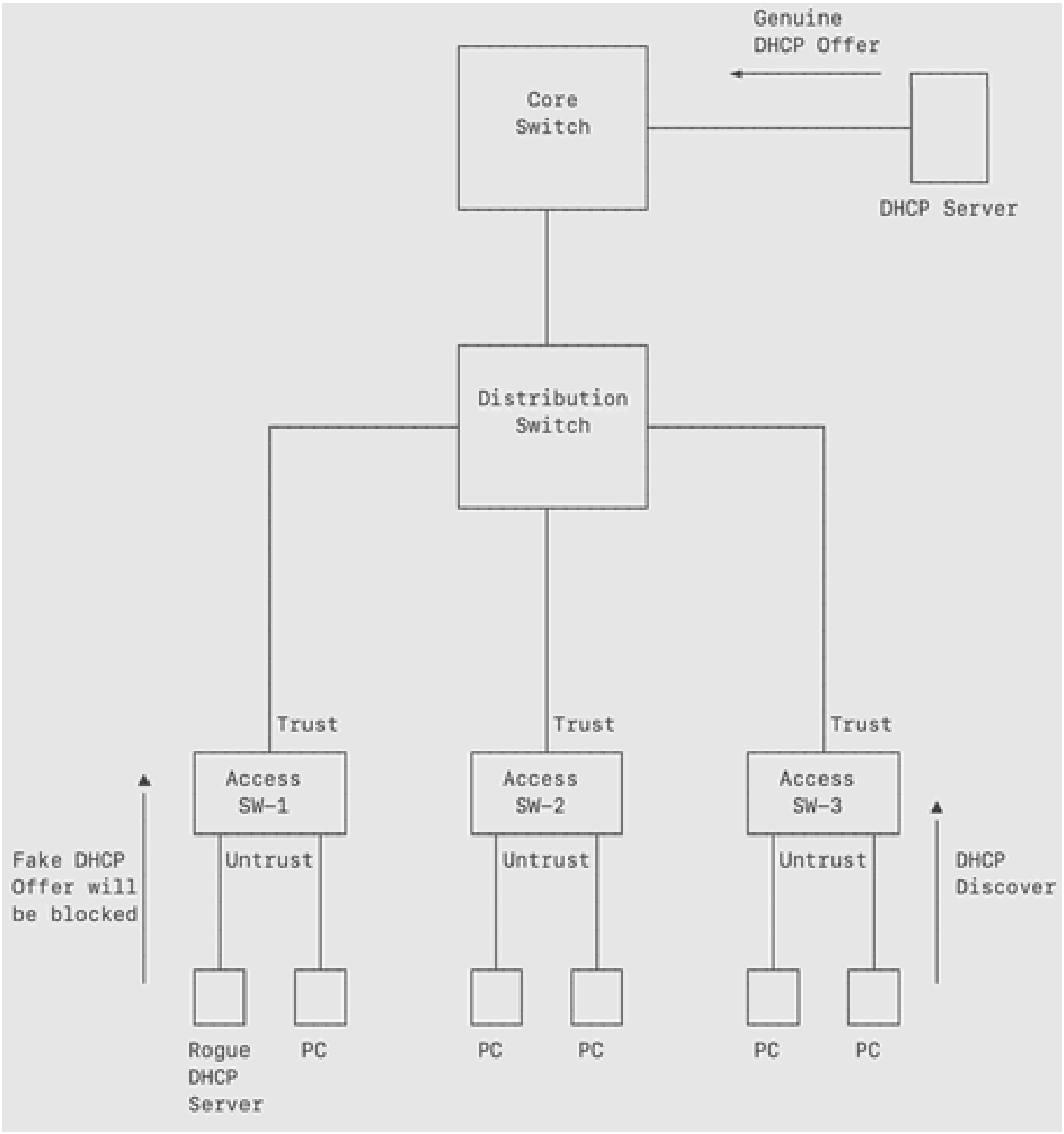
IPSG est une fonctionnalité de sécurité qui restreint le trafic IP sur les interfaces de couche 2 non routées en filtrant le trafic en fonction de la base de données de liaison de surveillance DHCP et des liaisons de source IP configurées manuellement. Vous pouvez utiliser IPSG pour empêcher les attaques de trafic si un hôte tente d'utiliser l'adresse IP de son voisin.

Scénario sans surveillance DHCP



1. Dans ce schéma, vous pouvez voir que plusieurs clients souhaitent recevoir une adresse IP du serveur DHCP connecté au commutateur principal.
2. Cependant, un serveur DHCP malveillant/non autorisé est connecté à l'un des commutateurs de couche d'accès qui peut recevoir les détections DHCP et envoyer les offres DHCP plus rapidement que le serveur DHCP réel.
3. Le pirate peut définir l'adresse de la passerelle dans le message d'offre de telle sorte qu'il puisse recevoir tout le trafic du client, compromettant ainsi la confidentialité de la communication.
4. C'est ce qu'on appelle l'attaque Man In The Middle.

Scénario avec surveillance DHCP

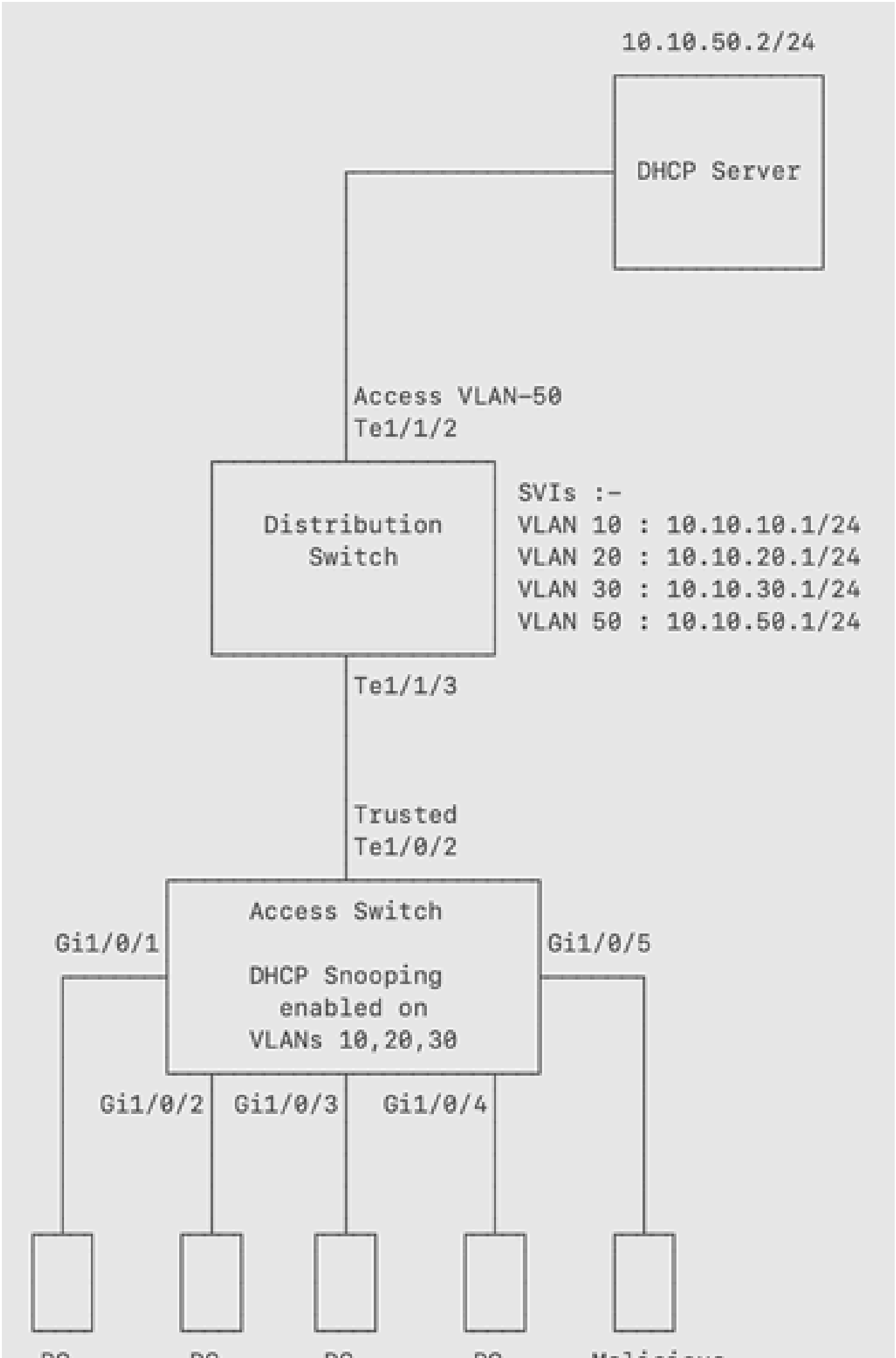


1. En activant la surveillance DHCP dans les commutateurs d’accès, configurez le commutateur pour écouter le trafic DHCP et arrêter tous les paquets DHCP malveillants qui sont reçus sur des ports non approuvés.
2. Dès que vous activez la surveillance DHCP dans le commutateur, toutes les interfaces deviennent automatiquement non fiables.
3. Conservez les ports connectés aux périphériques finaux non approuvés et configurez les ports connectés au serveur DHCP authentique comme étant approuvés.
4. Une interface non approuvée bloque les messages d’offre DHCP. Les messages d'offre DHCP

ne seront autorisés que sur les ports approuvés.
5. Vous pouvez limiter le nombre de paquets de détection DHCP que les hôtes finaux peuvent envoyer à une interface non approuvée par seconde. Il s'agit d'un mécanisme de sécurité destiné à protéger le serveur DHCP d'un nombre anormalement élevé de détections DHCP entrantes qui peuvent épuiser le pool en un rien de temps.

Dans cette section, il est expliqué comment configurer la surveillance DHCP dans un réseau commuté :

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
```

Étape 2. Configurez l'approbation de surveillance DHCP sur toutes les interfaces du commutateur d'accès qui reçoivent des offres DHCP de serveurs DHCP authentiques. Le nombre de ces interfaces dépend de la conception du réseau et de l'emplacement des serveurs DHCP. Ce sont les interfaces qui vont vers le serveur DHCP authentique.

Commutateur d'accès :

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

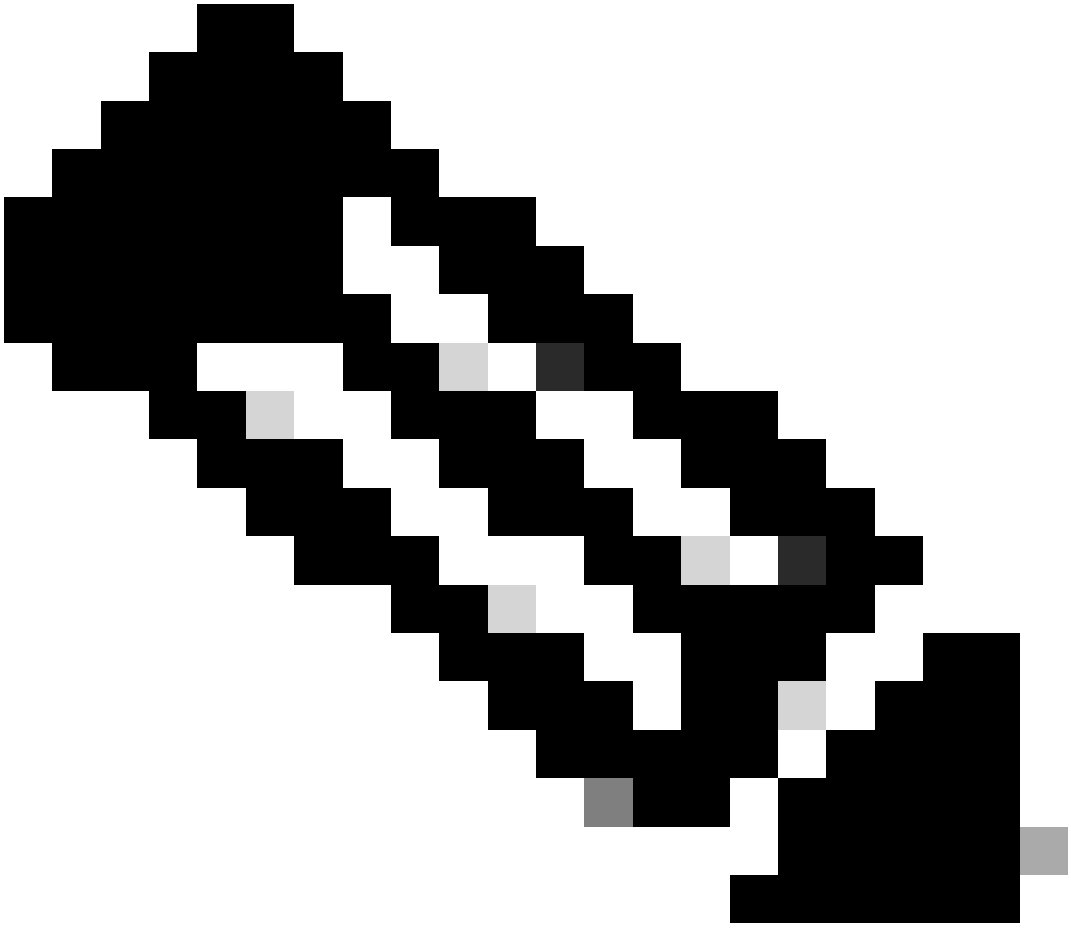
Étape 3. Une fois que vous avez configuré la surveillance DHCP globalement, tous les ports du commutateur ne sont plus approuvés automatiquement (à l'exception de ceux que vous approuvez manuellement, comme indiqué précédemment). Vous pouvez cependant configurer le nombre de paquets de détection DHCP que les hôtes finaux peuvent envoyer aux interfaces non approuvées par seconde.
Il s'agit d'un mécanisme de sécurité destiné à protéger le serveur DHCP d'un nombre anormalement élevé de détections DHCP entrantes qui peuvent épuiser le pool en un rien de temps.

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

Vérification :

```
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:
```



Remarque : si vous regardez cette sortie, vous voyez que Gi1/0/5 qui est connecté au serveur DHCP malveillant est mentionné dans la **show ip dhcp snooping** sortie comme non fiable.

Ainsi, la surveillance DHCP effectuera toutes ses vérifications sur ces ports.

Par exemple, toutes les offres DHCP entrantes sur ce port (Gi1/0/5) seront abandonnées.

Voici la table de liaison de la surveillance DHCP, montrant l'adresse IP, l'adresse MAC et l'interface pour 3 clients sur 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

À des fins de démonstration, ip dhcp snooping trust la configuration est supprimée sous Te1/0/2 dans le commutateur d'accès. Veuillez consulter les journaux générés dans le commutateur :

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

- Comme vous pouvez le voir, le commutateur d'accès abandonne les paquets d'offre DHCP entrants sur Te1/0/2 car il n'est plus approuvé.

- Les adresses MAC dans les journaux appartiennent aux interfaces SVI des VLAN 10, 20 et 30 car ce sont elles qui envoient ces offres du serveur DHCP à ces clients.

Empoisonnement ARP

Le protocole ARP assure la communication IP dans un domaine de diffusion de couche 2 en mappant une adresse IP à une adresse MAC. Il s'agit d'un protocole simple mais vulnérable à une attaque appelée empoisonnement ARP.

L’empoisonnement ARP est une attaque au cours de laquelle un pirate envoie de faux paquets de réponse ARP sur le réseau.

Un utilisateur malveillant peut attaquer les hôtes, les commutateurs et les routeurs connectés à votre réseau de couche 2 en empoisonnant les

caches ARP des systèmes connectés au sous-réseau et en interceptant le trafic destiné aux autres hôtes du sous-réseau

C'est l'attaque classique de l'homme du milieu.

Mécanismes de prévention

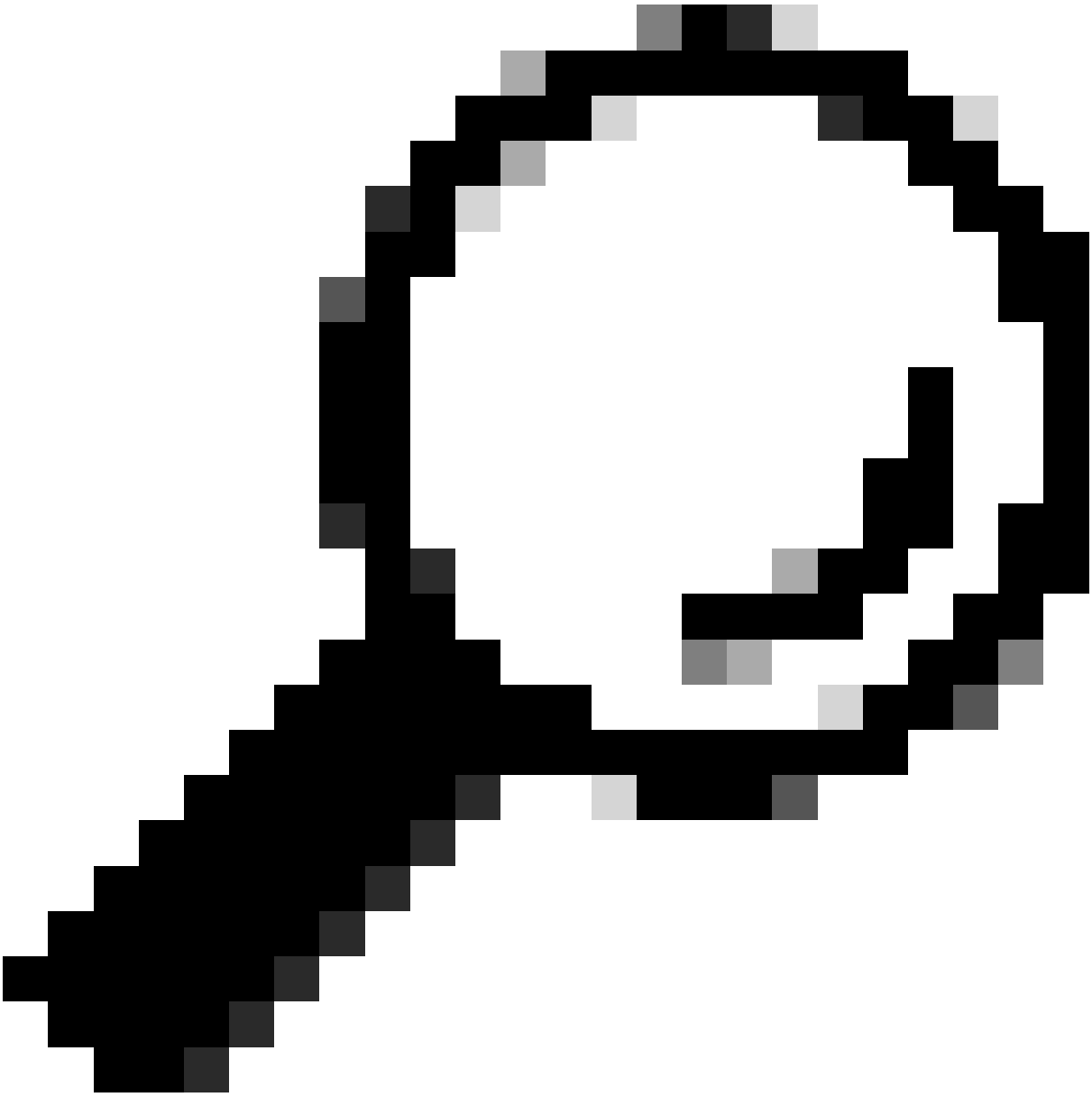
Inspection ARP dynamique (DAI)

L’inspection dynamique d’ARP est une fonction de sécurité qui valide les paquets ARP dans un réseau. Il intercepte, enregistre et rejette les paquets ARP ayant des liaisons d’adresses IP à MAC non valides. Cette fonction protège le réseau contre certaines attaques de l’homme du milieu.

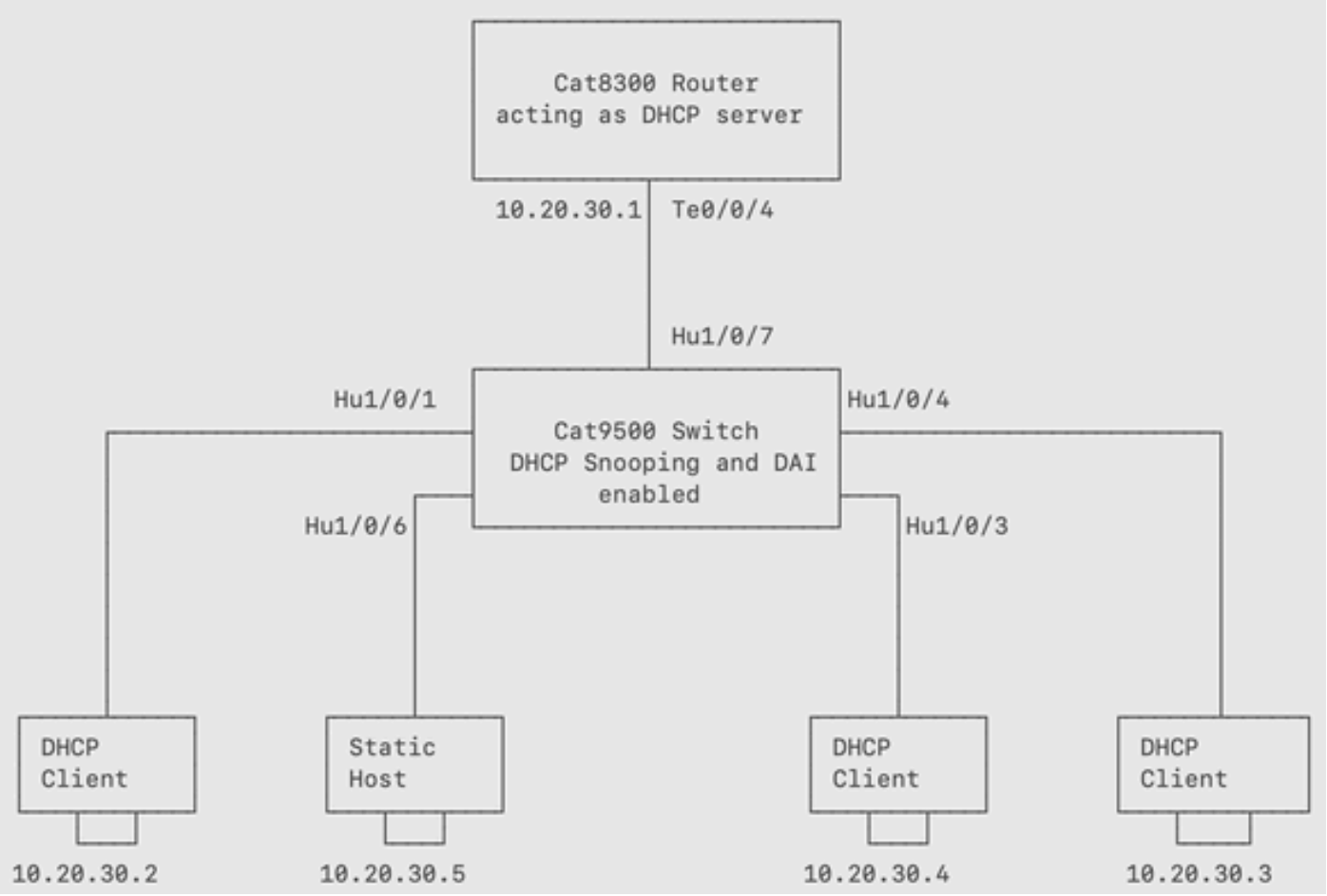
L’inspection dynamique d’ARP garantit que seules les requêtes et les réponses d’ARP valides sont relayées. Le commutateur effectue les activités suivantes :

- Il intercepte toutes les requêtes et les réponses ARP sur les ports non sécurisés.
- Vérifie que chacun de ces paquets interceptés a une liaison d'adresse IP à MAC valide avant de mettre à jour le cache ARP local ou avant de transférer le paquet à la destination appropriée
- Il abandonne les paquets ARP non valides.

L’inspection dynamique d’ARP détermine la validité d’un paquet ARP en fonction des liaisons d’adresses IP à MAC valides stockées dans une base de données sécurisée, la base de données de liaison d’espionnage DHCP.
Cette base de données est créée par l’espionnage DHCP si ce dernier est activé sur les réseaux VLAN et le commutateur. Si le paquet ARP entre sur une interface sécurisée, le commutateur le transfère sans vérification.
Sur les interfaces non sécurisées, le commutateur transmet le paquet uniquement s’il est valide.



Conseil : reportez-vous à 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



Cette image montre un commutateur Cat9500 connecté à quatre hôtes, dont 3 hôtes sont des clients DHCP et 1 hôte a une adresse IP statique (10.20.30.5). Le serveur DHCP est un routeur de la gamme Cat8300 configuré avec un pool DHCP.

La topologie ci-dessus est utilisée pour démontrer comment DAI détecte les requêtes ARP non valides sur une interface et protège le réseau contre les attaques malveillantes.

Configuration:

Étape 1. Configurez la surveillance DHCP et le DAI globalement dans le commutateur.

```
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
```

Étape 2. Configurez l'interface Hu1/0/7 qui est connectée au serveur DHCP en tant que port sécurisé. Cela permettra aux offres DHCP d'entrer dans l'interface et d'atteindre ensuite les clients DHCP.

```
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
```

Étape 3. Configurez les ports connectés aux clients DHCP en tant que ports d'accès autorisant le 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
```

Étape 4. Vérifiez si les clients DHCP ont reçu une adresse IP du serveur DHCP, à partir de la table de liaison de surveillance DHCP dans le commutateur Cat9500.

```
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
```

Vous pouvez également vérifier les liaisons dans le serveur DHCP.

```
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

Étape 5 : Changez l'adresse IP de l'hôte connecté à Hu1/0/6 de 10.20.30.5 à 10.20.30.2 et essayez d'envoyer une requête ping aux autres clients DHCP à partir de cet hôte.

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:
.....

Ces journaux ARP non valides sont visibles sur le commutateur Cat9500 :

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

- Comme vous pouvez le voir, lorsque vous essayez d'envoyer une requête ping vers 10.20.30.3 et 10.20.30.4 à partir de Static_Host, vous ne pouvez pas le faire.
  Bien que Static_Host ait tenté d'usurper l'adresse IP du client DHCP légitime, il n'a pas pu le faire car tout paquet ARP qui arrive sur Hu1/0/6 sera inspecté par le commutateur et comparé aux données présentes dans la table de liaison de surveillance DHCP.

- Les journaux suivants du commutateur Cat9500 confirment que les requêtes ARP envoyées par l'hôte statique aux clients DHCP sont abandonnées.

- Pour ce faire, le commutateur Cat9500 se réfère à la base de données de liaison de surveillance DHCP.

- Lorsqu'une requête ARP entre dans Hu1/0/6 avec l'adresse MAC-IP source qui ne correspond pas aux valeurs présentes dans la base de données de liaison de surveillance DHCP, le commutateur abandonne la requête ARP.

Étape 6. Vérification :

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

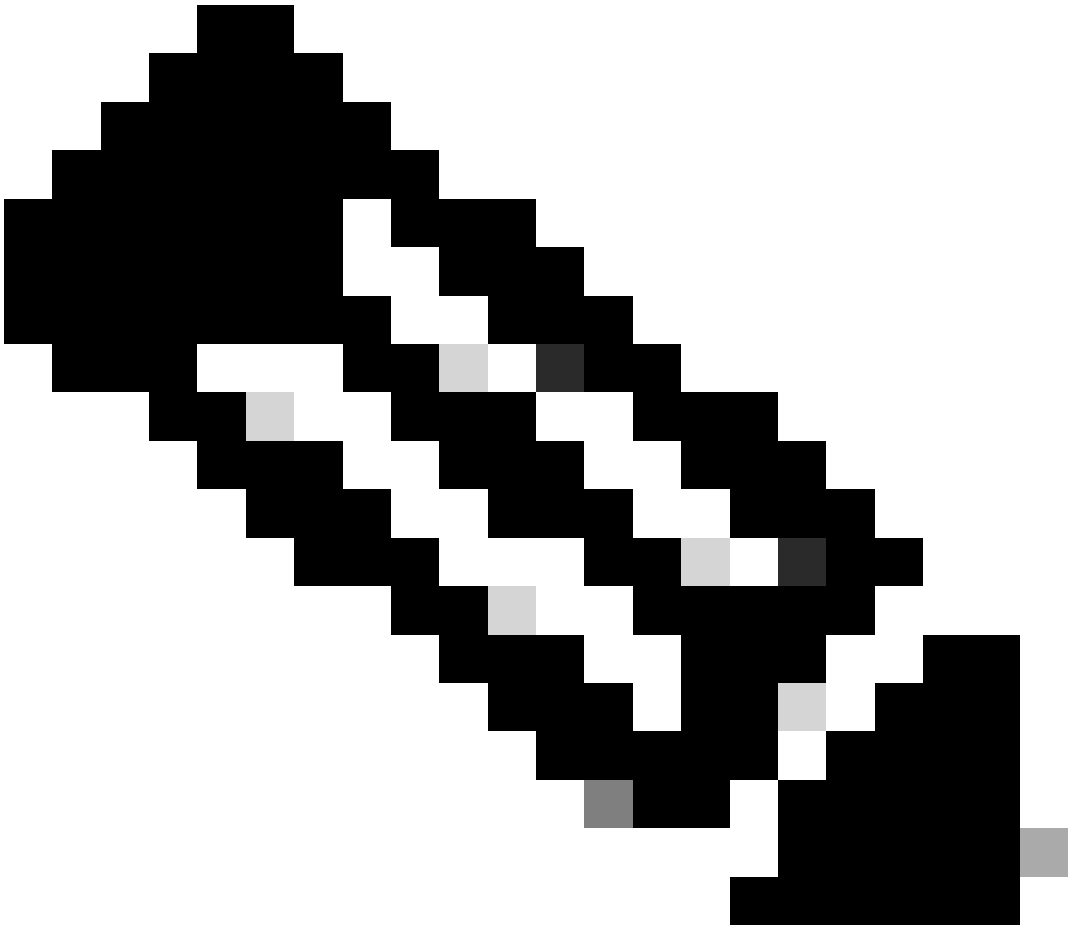
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures
10	6	3	0	0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data

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

10 0 0 0

Dans ce résultat, vous pouvez voir le nombre de paquets abandonnés et autorisés par DAI dans VLAN 10 dans le commutateur Cat9500.



Remarque : un scénario très important peut être un hôte légitime du réseau auquel est attribuée une adresse IP statique (par exemple 10.20.30.5) ?

Bien que l'hôte n'essaie pas d'usurper quoi que ce soit, il est toujours isolé du réseau car ses données de liaison MAC-IP ne sont pas présentes dans la base de données de liaison de surveillance DHCP.

En effet, l'hôte statique n'a jamais utilisé DHCP pour recevoir l'adresse IP, car elle lui a été attribuée de manière statique.

Nous avons quelques solutions de contournement qui peuvent être implémentées pour fournir la connectivité aux hôtes légitimes qui ont des adresses IP statiques.

Option 1.

Configurez l’interface connectée à l’hôte avec la confiance d’inspection ip arp.

```
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.

Autorisez l'hôte statique à l'aide d'une liste d'accès ARP :

```
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.

Configurez une entrée de table de liaison pour l'hôte statique.

```
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
```

Options supplémentaires disponibles avec 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
```

Pour src-mac, vérifiez l'adresse MAC source dans l'en-tête Ethernet par rapport à l'adresse MAC de l'expéditeur dans le corps ARP. Cette vérification est effectuée à la fois sur les requêtes et les réponses ARP. Lorsque cette option est activée, les paquets avec des adresses MAC différentes sont classés comme non valides et sont abandonnés

Pour dst-mac, vérifiez l'adresse MAC de destination dans l'en-tête Ethernet par rapport à l'adresse MAC cible dans le corps ARP. Cette vérification est effectuée pour les réponses ARP. Lorsque cette option est activée, les paquets avec des adresses MAC différentes sont classés comme non valides et sont abandonnés.

Pour IP, recherchez les adresses IP incorrectes et inattendues dans le corps ARP. Les adresses incluent 0.0.0.0, 255.255.255.255 et toutes les adresses de multidiffusion IP. Les adresses IP des expéditeurs sont vérifiées dans toutes les requêtes et réponses ARP, et les adresses IP cibles sont vérifiées uniquement dans les réponses ARP.

Vous pouvez également configurer la limitation du débit ARP. Par défaut, il y a une limite de 15 pps pour le trafic ARP sur les interfaces non approuvées :

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

Protection de la source IP

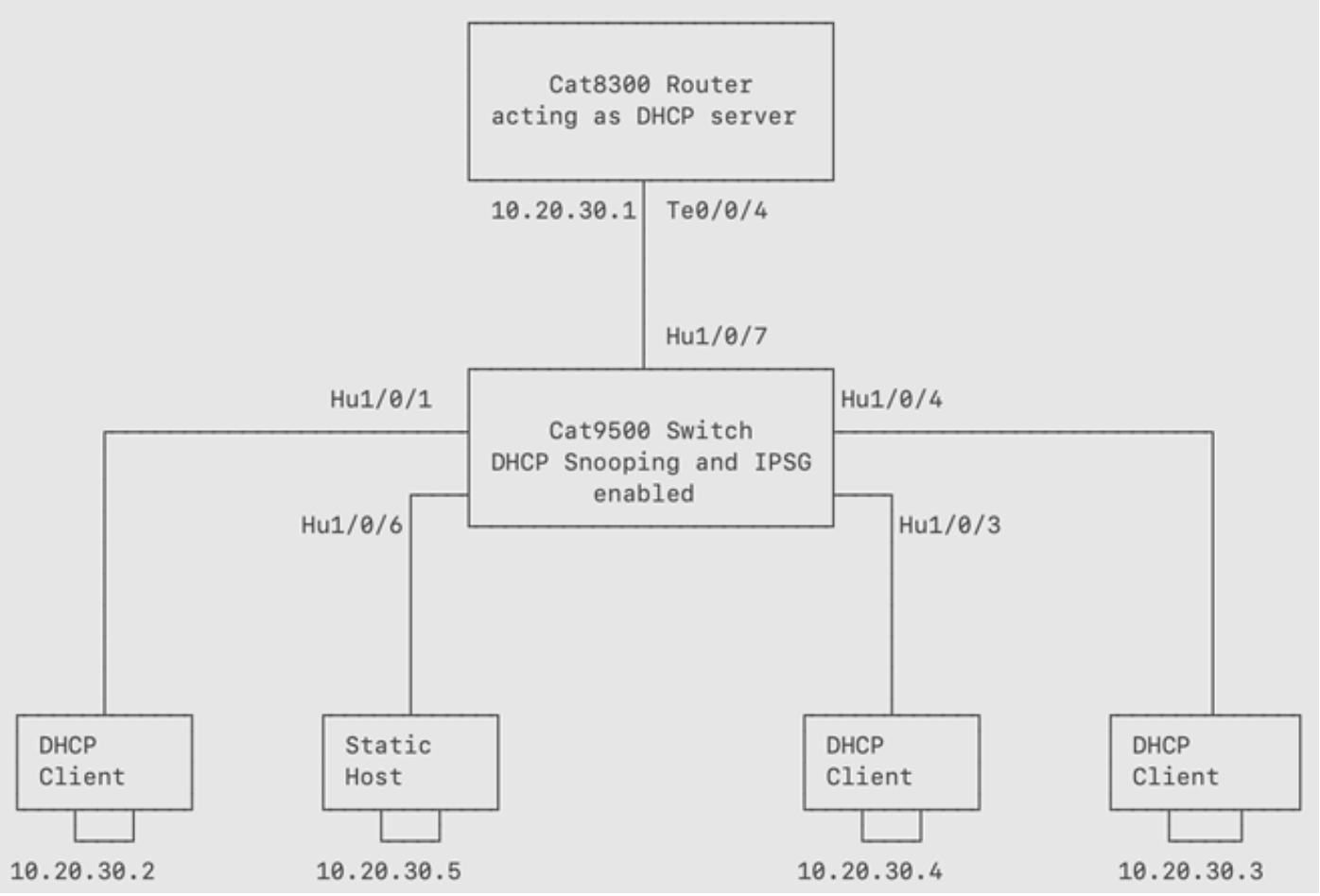
- IPSG est une fonctionnalité de sécurité qui restreint le trafic IP sur les interfaces de couche 2 non routées en filtrant le trafic en fonction de la base de données de liaison de surveillance DHCP et des liaisons de source IP configurées manuellement.
- Vous pouvez utiliser IPSG pour empêcher les attaques de trafic si un hôte tente d'utiliser l'adresse IP de son voisin.
- Vous pouvez activer IPSG lorsque la surveillance DHCP est activée sur une interface non approuvée. Une fois que le protocole IPSG est activé sur une interface, le commutateur bloque tout le trafic IP reçu sur l'interface, à l'exception des paquets DHCP autorisés par la surveillance DHCP.
- Le commutateur utilise une table de recherche IP source dans le matériel pour lier les adresses IP aux ports. Pour le filtrage IP et MAC, une combinaison d'adresses IP source et de recherches MAC source est utilisée. Le trafic IP avec une adresse IP source dans la table de liaison est autorisé, tout autre trafic est refusé.
- La table de liaison de la source IP comporte des liaisons qui sont enregistrées par l'espionnage DHCP ou qui sont configurées manuellement (liaisons de source IP statiques). Une entrée figurant dans cette table comporte une adresse IP, son adresse MAC associée ainsi que son numéro de VLAN correspondant. Le commutateur utilise la table de liaison de la source IP uniquement lorsque la protection de la source IP est activée.
- Vous pouvez configurer IPSG avec le filtrage des adresses IP source ou avec le filtrage des adresses IP source et MAC.

IPSG pour les hôtes statiques

- IPSG pour les hôtes statiques permet à IPSG de fonctionner sans DHCP. IPSG pour les hôtes statiques utilise les entrées de la table de suivi des périphériques IP pour installer les listes de contrôle d'accès des ports. Le commutateur crée des entrées statiques basées sur des requêtes ARP ou d'autres paquets IP pour gérer la liste des hôtes valides pour un port donné.

Référence:

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



Le commutateur Cat9500 est connecté à quatre hôtes, dont trois hôtes sont des clients DHCP et un hôte a une adresse IP statique. Le serveur DHCP est un routeur de la gamme Cat8300 configuré avec un pool DHCP.
Vous pouvez utiliser cette topologie pour démontrer comment IPSG détecte et bloque le trafic provenant d'hôtes dont les liaisons MAC-IP ne sont pas présentes dans la base de données de liaison de surveillance DHCP.

Configurer:

Étape 1. Configurez la surveillance DHCP globalement dans le commutateur Cat9500.

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

Étape 2. Configurez l'interface Te1/0/7 qui est connectée au serveur DHCP en tant que port sécurisé. Cela permet aux offres DHCP d'entrer dans l'interface et d'atteindre ensuite les clients DHCP.

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
```

Étape 3. Configurez les ports connectés aux clients DHCP en tant que ports d'accès autorisant le 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
```

Étape 4. Vérifiez si les clients DHCP ont reçu l'adresse IP du serveur DHCP.

```
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

Étape 5. Configurez IPSG sous les interfaces connectées à tous les hôtes finaux (3 clients DHCP et 1 hôte avec une adresse IP statique).

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
```

Vérification :

```
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
```

À partir de ce résultat, vous pouvez voir que le champ d'adresse IP est défini sur deny-all pour Hu1/0/6 car il n'y a aucune liaison MAC-IP correspondant à cette interface dans la table de liaison de surveillance DHCP.

Étape 6. Essayez d'envoyer une requête ping aux clients DHCP avec les adresses IP 10.20.30.2, 10.20.30.3 et 10.20.30.4 à partir de l'hôte statique 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 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

Options supplémentaires disponibles avec IPSG :

Par défaut, IPSG filtre le trafic entrant sur les ports non approuvés en se basant uniquement sur les adresses IP.

Si vous souhaitez effectuer le filtrage en fonction des adresses IP et MAC, procédez comme suit.

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
```

Dans cette sortie, vous pouvez voir que le type de filtre est ip-mac. Ainsi, le commutateur filtre désormais les paquets entrants sur ces interfaces en fonction des adresses IP et MAC source.

Conseils de dépannage pour DAI et IPSG

- La première chose à vérifier lors du dépannage des problèmes DAI et IPSG est de vérifier si la table de liaison de surveillance DHCP a été correctement remplie.

- Avant d'activer ces fonctionnalités, gérez les points d'extrémité avec des adresses IP statiques. Si vous ne voulez pas que ces périphériques perdent leur accessibilité, configurez des liaisons statiques ou utilisez l'une des méthodologies mentionnées précédemment pour que le commutateur fasse confiance à ces points d'extrémité.

- Lors de la configuration de DAI ou IPSG dans un environnement où la surveillance DHCP n'est pas déjà activée et où les clients ont déjà reçu des adresses IP du serveur DHCP, activez d'abord la surveillance DHCP et effectuez l'une des deux étapes suivantes :

    - Renvoi des interfaces connectées au client afin qu'elles renouvellent leur bail.

    - Attendez que les clients renouvellent automatiquement leur bail. Cela peut prendre plus de temps, mais vous évite de rebondir manuellement tous les ports connectés au client.

- L'exécution de l'une des deux étapes ci-dessus déclenchera une nouvelle transaction DORA. Le commutateur détecte les paquets DORA et met à jour la table de liaison. Si cela n'est pas fait et que le DAI ou l'IPSG est immédiatement activé après la configuration de la surveillance DHCP, vous risquez de rencontrer un problème où tous les clients DHCP du réseau perdent la connectivité au réseau.

- Lors du dépannage des problèmes de connectivité dans un environnement où DAI ou IPSG est configuré, assurez-vous que la table de liaison de surveillance DHCP n'est pas endommagée. Assurez-vous que le commutateur peut accéder à la structure de données dans laquelle cette table est stockée.

- Il peut y avoir des cas où la table de liaison est exportée vers un support qui prend du temps à être initialisé après le démarrage du commutateur ou devient inaccessible au commutateur pour une raison quelconque. Vous avez peut-être observé des problèmes de connectivité dans de tels scénarios.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.