Catalystスイッチにおけるダイナミックarpインスペクション(DAI)とIPソースガード(IPSG)のトラブルシューティング

内容

はじめに

このドキュメントでは、ダイナミックARPインスペクション(DAI)とIPソースガード(IPSG)の動作方法と、Catalyst 9Kスイッチでこれらの機能を検証する方法について説明します。

DHCPスヌーピングおよび関連機能

DAIとIPSGについて詳しく調べる前に、DAIとIPSGの前提条件であるDHCPスヌーピングについて簡単に説明する必要があります。

Dynamic Host Configuration Protocol(DHCP)は、インターネットプロトコル(IP)ホストに対して、そのIPアドレスと、サブネットマスクやデフォルトゲートウェイなどのその他の関連する設定情報を自動的に提供するクライアント/サーバプロトコルです。RFC 2131および2132では、DHCPはブートストラッププロトコル(BOOTP)に基づくインターネット技術特別調査委員会(IETF)標準として定義されています。BOOTPは、DHCPが多くの実装詳細を共有するプロトコルです。DHCPを使用すると、ホストは必要なTCP/IP設定情報をDHCPサーバから取得できます。

DHCPスヌーピングは、信頼できないホストと信頼できるDHCPサーバの間のファイアウォールのように動作するセキュリティ機能です。DHCPスヌーピング機能は、次のアクティビティを実行します。

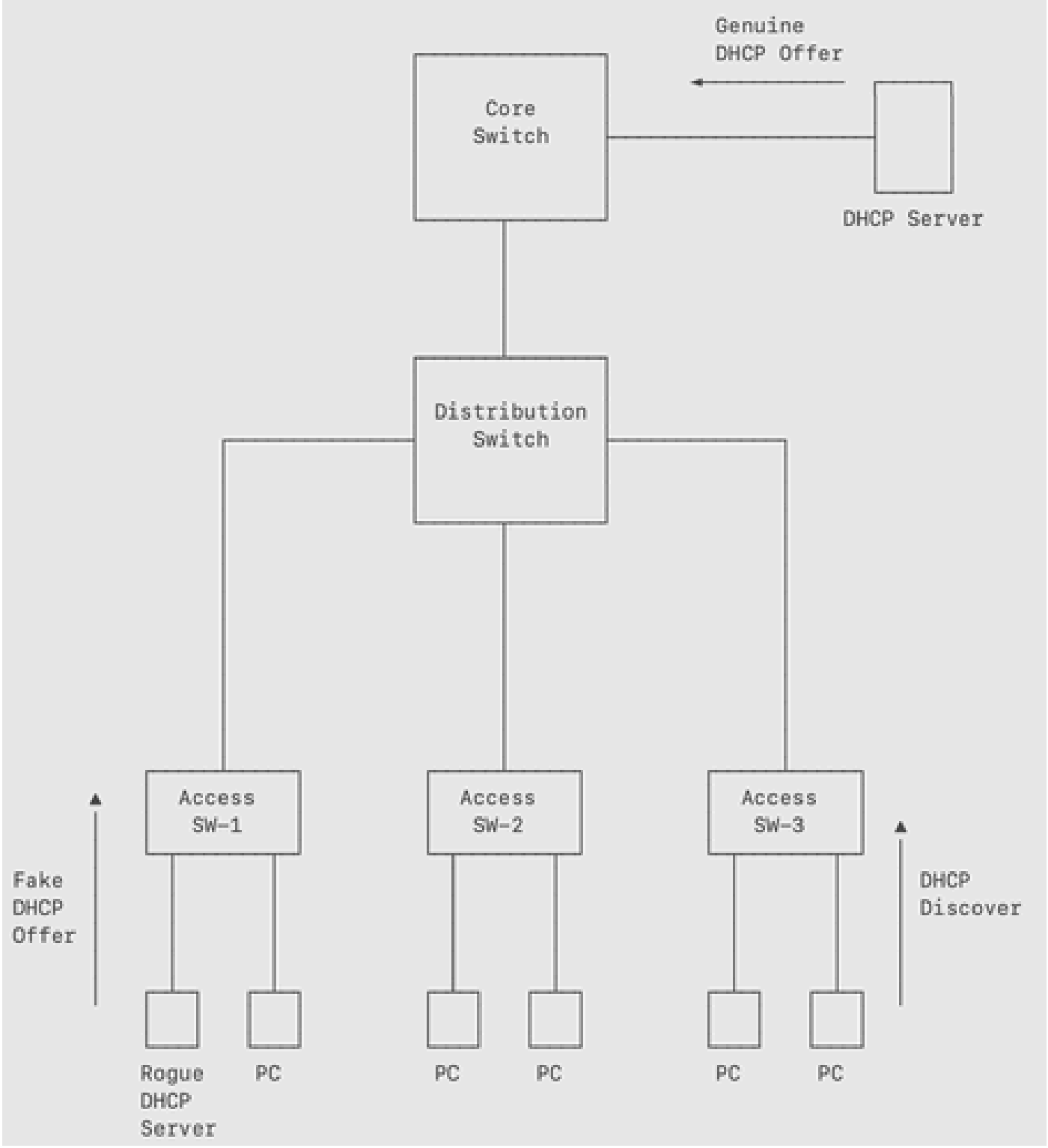
- 信頼できない送信元から受信したDHCPメッセージを検証し、無効なメッセージを除外します。
- 信頼できる発信元と信頼できない発信元からのDHCPトラフィックをレート制限します。
- DHCPスヌーピングバインディングデータベースを構築および維持します。このデータベー

スには、リースされたIPアドレスを持つ信頼できないホストに関する情報が含まれます。
- DHCPスヌーピングバインディングデータベースを使用して、信頼できないホストからの後続の要求を検証します。

DAIは、ネットワーク内のアドレス解決プロトコル(ARP)パケットを検証するセキュリティ機能です。DAIを使用すると、ネットワーク管理者は、IPアドレスバインディングへの無効なMACアドレスを持つARPパケットを代行受信、ロギング、および廃棄できます。この機能は、特定の「中間者攻撃」からネットワークを保護します。

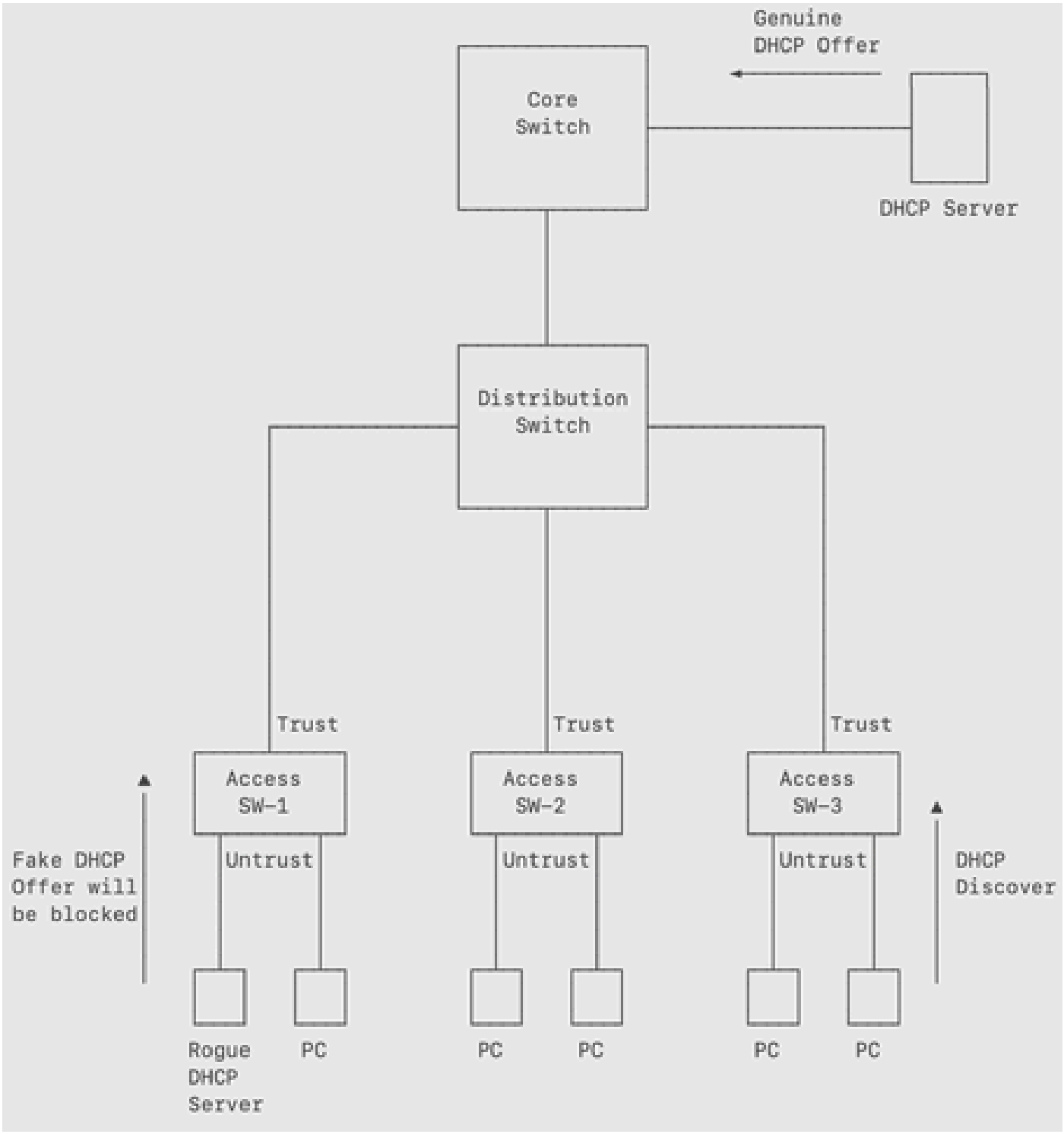
IPSGは、非ルーテッドレイヤ2インターフェイス上のIPトラフィックを制限するセキュリティ機能で、DHCPスヌーピングバインディングデータベースおよび手動で設定されたIPソースバインディングに基づいてトラフィックをフィルタリングします。ホストがネイバーのIPアドレスを使用しようとする場合は、IPSGを使用してトラフィック攻撃を防止できます。

DHCPスヌーピングを使用しないシナリオ



1. この図では、複数のクライアントがコアスイッチに接続されたDHCPサーバからIPアドレスを受け取ることを望んでいることがわかります。
2. ただし、DHCPが実際のDHCPサーバよりも速くDHCPオファーを検出して送信できるアクセスレイヤスイッチの1つに接続された悪意のある/不正なDHCPサーバがあります。
3. 攻撃者は、クライアントからのすべてのトラフィックを受信できるようにオファーメッセージにゲートウェイアドレスを設定できるため、通信の機密性を損なう可能性があります。
4. これは中間者攻撃として知られています。

DHCPスヌーピングのシナリオ

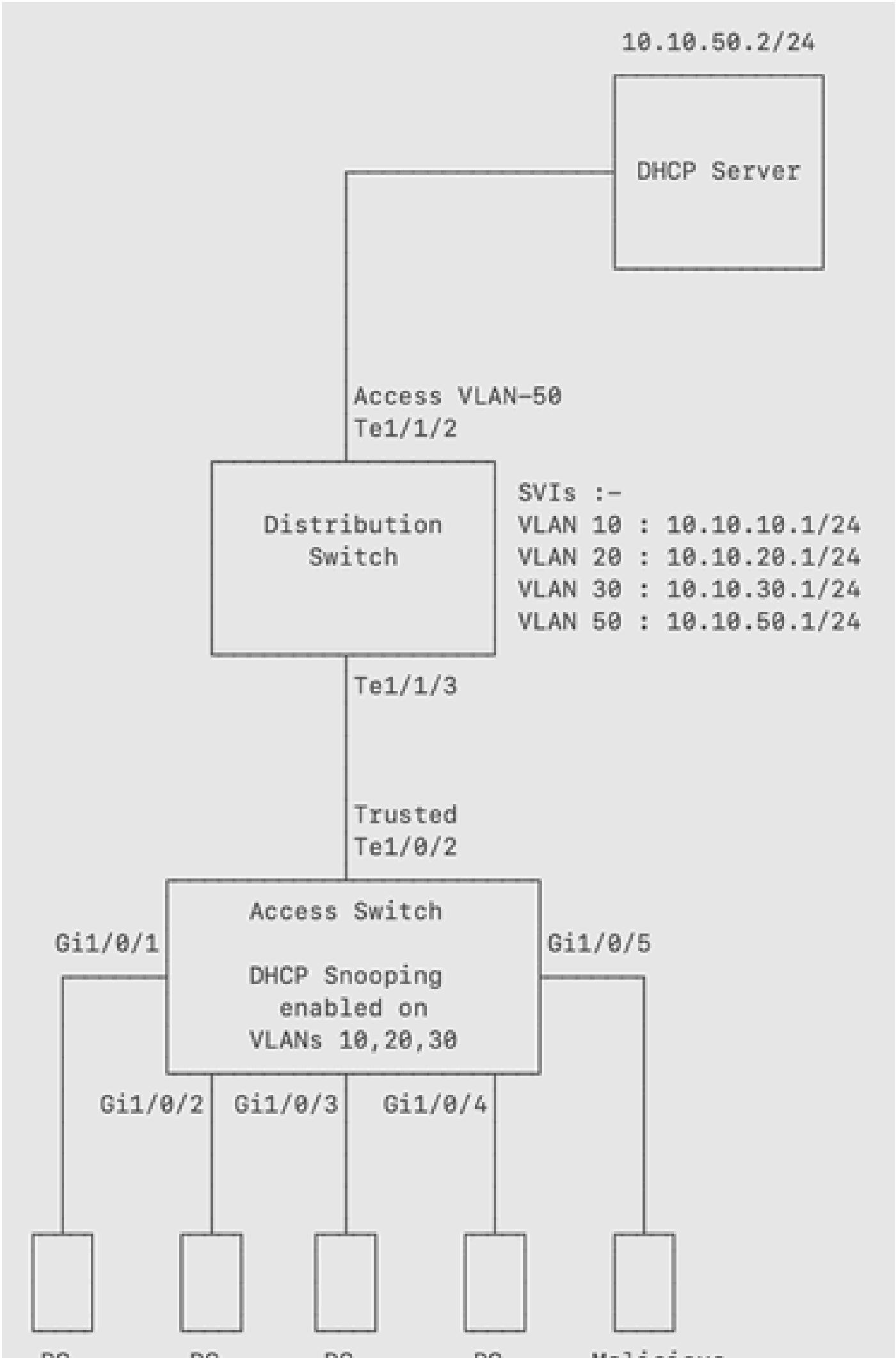


1. アクセススイッチでDHCPスヌーピングを有効にして、DHCPトラフィックを受信するようにスイッチを設定し、信頼できないポートで受信される悪意のあるDHCPパケットを停止します。
2. スイッチでDHCPスヌーピングを有効にするとすぐに、すべてのインターフェイスが自動的に信頼できない状態になります。
3. エンドデバイスに接続されているポートを信頼できない状態に保ち、正規のDHCPサーバに接続されているポートを信頼できるポートとして設定します。
4. 信頼できないインターフェイスはDHCPオファーメッセージをブロックします。DHCPオファーメッセージは、信頼できるポートでのみ許可されます。

5. エンドホストが信頼できないインターフェイスに送信できるDHCP検出パケットの1秒あたりの数を制限できます。 これは、短時間でプールを枯渇させる可能性がある異常に多数の着信DHCP検出からDHCPサーバを保護するためのセキュリティメカニズムです。

このセクションでは、スイッチドネットワークでDHCPスヌーピングを設定する方法について説明します。

トポロジ：


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
```

ステップ 2：正規のDHCPサーバからDHCPオファーを受信するアクセススイッチのすべてのインターフェイスでDHCPスヌーピング信頼を設定します。このようなインターフェイスの数は、ネットワークの設計とDHCPサーバの配置によって異なります。これらは、正規のDHCPサーバに向かうインターフェイスです。

アクセススイッチ：

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

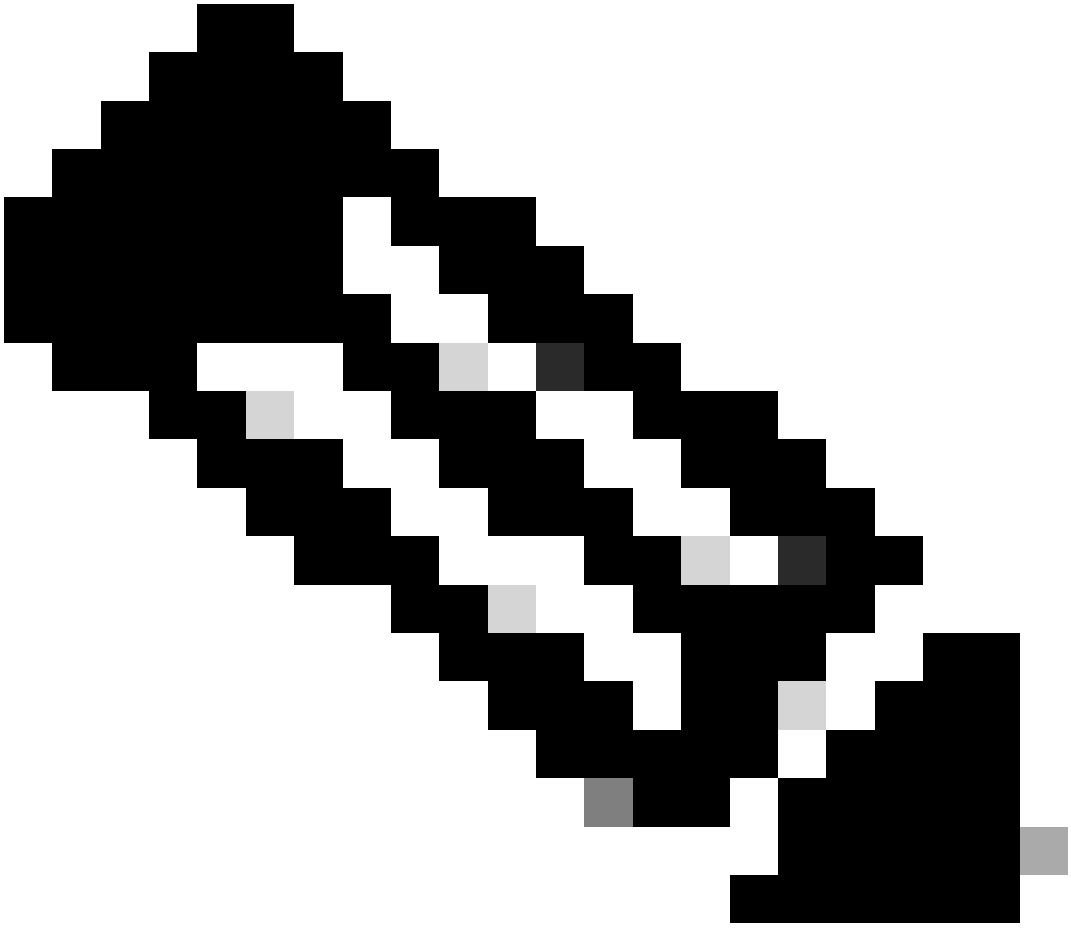
ステップ 3：DHCPスヌーピングをグローバルに設定すると、スイッチ内のすべてのポートは自動的に信頼できないポートになります（前に示したように、手動で信頼できるポートを除く）。ただし、エンドホストが信頼できないインターフェイスに送信できるDHCP検出パケットの1秒あたりの数を設定できます。
これは、短時間でプールを枯渇させる可能性がある異常に多数の着信DHCP検出からDHCPサーバを保護するためのセキュリティメカニズムです。

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

検証：

```
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:
```



注：この出力を見ると、悪意のあるDHCPサーバに接続されているGi1/0/5が**show ip dhcp snooping** の出力で信頼できないとして示されていることがわかります。

したがって、DHCPスヌーピングはこれらのポートですべてのチェックを行います。
たとえば、これにより、このポート(Gi1/0/5)のすべての着信DHCPオファーがドロップされます。

DHCPスヌーピングバインディングテーブルを次に示します。これはGi1/0/1、Gi1/0/2、Gi1/0/3上の3つのクライアントのIPアドレス、MACアドレス、およびインターフェイスを示しています。

```
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

説明のため、アクセススイッチのTe1/0/2の下からip dhcp snooping trust configを削除します。Switch：プロンプトで生成されたログを

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

- アクセススイッチは信頼できなくなったため、Te1/0/2の着信DHCPオファーパケットをドロップしていることがわかります。
- ログ内のMACアドレスはVLAN 10、20、および30のSVIに属しています。これらのMACアドレスは、DHCPサーバからこれらのクライアントにオファーを送信するアドレスであるためです。

ARPポイズニング

ARPは、IPアドレスをMACアドレスにマッピングすることによって、レイヤ2ブロードキャストドメイン内のIP通信を提供します。これは単純なプロトコルですが、ARPポイズニングと呼ばれる攻撃に対しては脆弱です。

ARPポイズニングは、攻撃者がネットワーク上で偽のARP応答パケットを送信する攻撃です。

悪意のあるユーザは、サブネットに接続されているシステムのARPキャッシュをポイズニングし、サブネット上の他のホスト宛て

のトラフィックを傍受することで、レイヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃する可能性があります

これは古典的な中間者攻撃です。

予防メカニズム

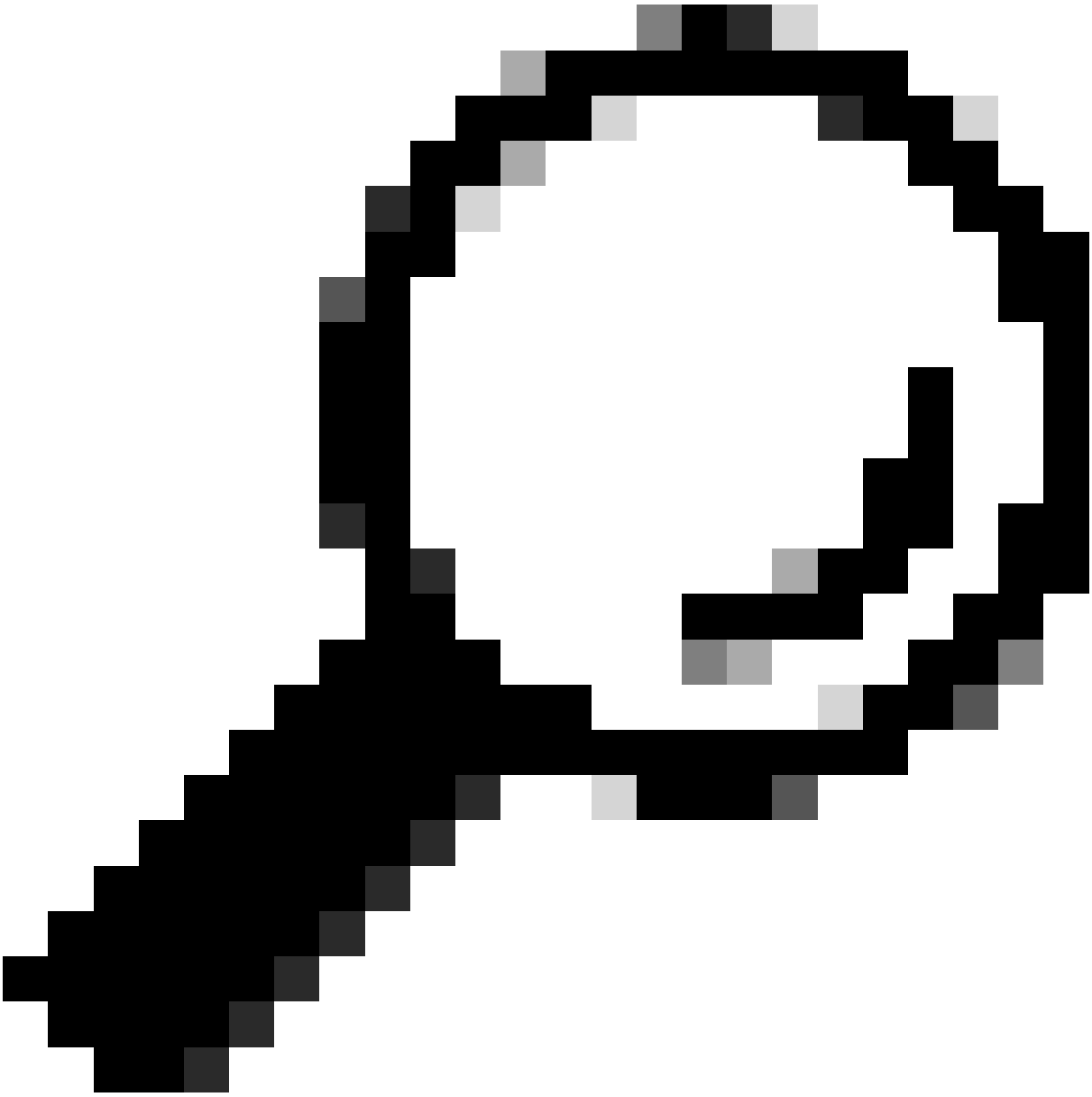
ダイナミックARPインスペクション(DAI)

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットを検証するセキュリティ機能です。無効な IP から MAC へのアドレス バインディングを持つ ARP パケットを捕捉、ログ記録、および廃棄します。この機能は、ある種の中間者攻撃からネットワークを保護します。

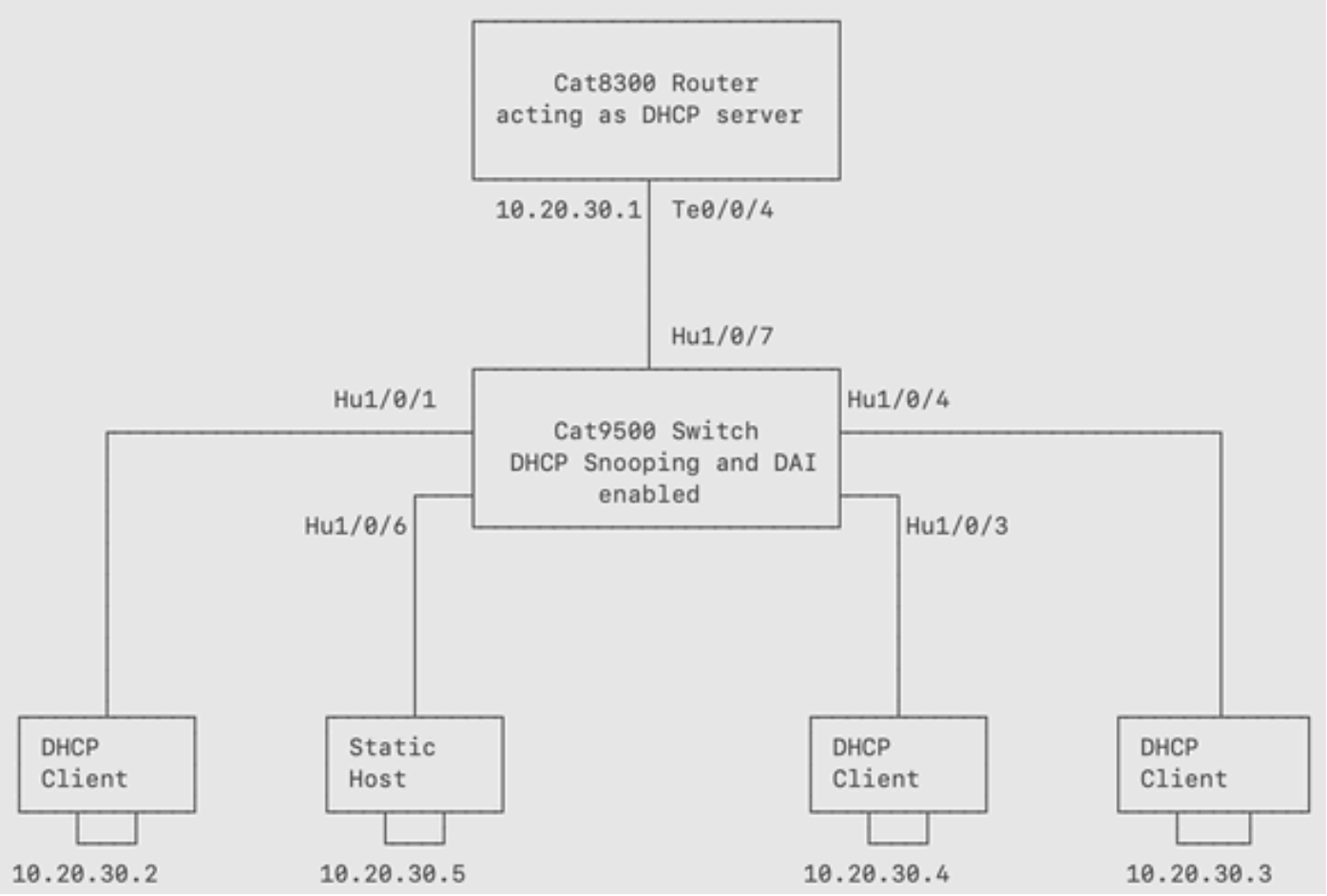
ダイナミック ARP インスペクションにより、有効な ARP 要求および応答のみがリレーされるようになります。スイッチは次の動作を実行します。

- 信頼できないポート上のすべての ARP 要求および応答を捕捉する
- ローカルARPキャッシュを更新する前、またはパケットを適切な宛先に転送する前に、これらの代行受信された各パケットに有効なIPからMACへのアドレスバインディングがあることを確認します
- 無効な ARP パケットを廃棄する

ダイナミック ARP インスペクションは、信頼できるデータベースつまり DHCP スヌーピング バインディング データベースに格納されている有効な IP から MAC へのアドレス バインディングに基づいて、ARP パケットの有効性を判別します。
DHCP スヌーピングが VLAN およびスイッチ上で有効になっている場合、このデータベースは DHCP スヌーピングにより構築されます。信頼できるインターフェイス上で ARP パケットが受信された場合、スイッチはチェックを行うことなくそのパケットを転送します。
信頼できないインターフェイス上では、スイッチはパケットが有効である場合にのみパケットを転送します。



ヒント: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



次の図は、4台のホストに接続されたCat9500スイッチを示しています。この中の3台のホストはDHCPクライアントで、1台のホストは固定IPアドレス(10.20.30.5)を持っています。DHCPサーバは、DHCPプールを使用して設定されたCat8300シリーズルータです。

上記のトポロジは、DAIがインターフェイス上で無効なARP要求を検出し、悪意のある攻撃者からネットワークを保護する方法を示すために使用されます。

設定：

ステップ 1：DHCPスヌーピングとDAIをスイッチでグローバルに設定します。

```
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
```

ステップ 2：DHCPサーバに接続されているインターフェイスHu1/0/7を信頼できるポートとして設定します。これにより、DHCPオファーはインターフェイスに入力し、続いてDHCPクライアントに到達できます。

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

ステップ 3：DHCPクライアントに接続されているポートを、VLAN 10を許可するアクセスポートとして設定します。

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
```

ステップ 4：Cat9500スイッチのDHCPスヌーピングバインディングテーブルから、DHCPクライアントがDHCPサーバからIPアドレスを受信したかどうかを確認します。

```
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サーバのバインディングを確認することもできます。

```
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

ステップ5:Hu1/0/6に接続されているホストのIPアドレスを10.20.30.5から10.20.30.2に変更し、そのホストから他のDHCPクライアントにpingを実行します。

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

次の無効なARPログは、Cat9500スイッチで確認できます。

```
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
```

- Static_Hostから10.20.30.3と10.20.30.4にpingを実行しようとしても、実行できないことがわかります。Static_Hostが正規のDHCPクライアントのIPアドレスをスプーフィングしようとしましたが、Hu1/0/6に到達するARPパケットはスイッチによって検査され、DHCPスヌーピングバインディングテーブルにあるデータと比較されるため、スプーフィングできませんでした。

- Cat9500スイッチからの後続のログでは、Static_HostからDHCPクライアントに送信されているARP要求がドロップされていることを確認します。

- Cat9500スイッチは、DHCPスヌーピングバインディングデータベースを参照することでこれを実現します。

- ARP要求が、DHCPスヌーピングバインディングデータベースに存在する値と一致しない発信元MAC-IPを使用してHu1/0/6に入ると、スイッチはARP要求をドロップします。

手順 6：検証：

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

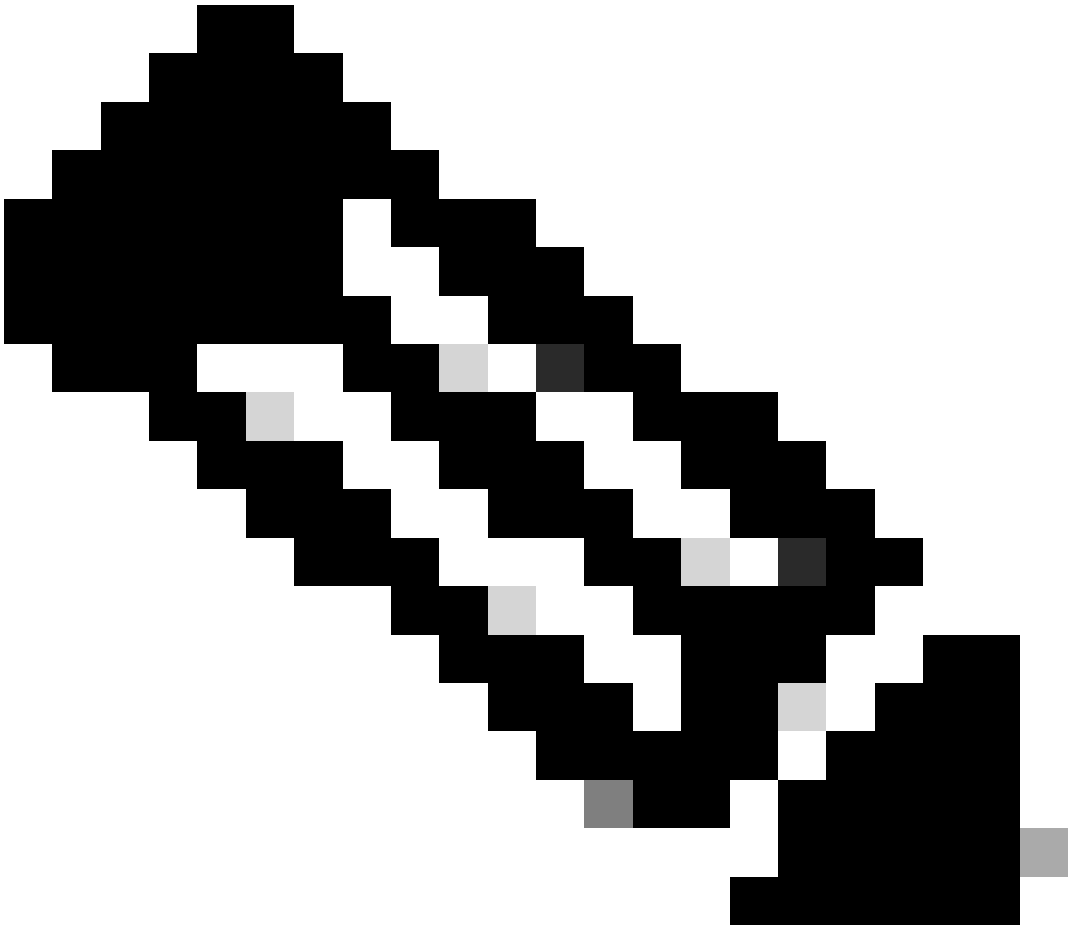
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures
10	6	3	0	0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data

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

10 0 0 0

この出力では、Cat9500スイッチでVLAN 10のDAIによって廃棄および許可されたパケットの数を確認できます。



注：非常に重要なシナリオの1つは、固定IPアドレス(10.20.30.5)アドレスが割り当てられた正規のホストです。

ホストは何もスプーフィングしようとしませんが、MAC-IPバインディングデータがDHCPスヌーピングバインディングデータベースにないため、ネットワークから分離されます。

これは、静的ホストが静的に割り当てられたため、静的ホストがDHCPを使用してIPアドレスを受信しなかったためです。

静的IPアドレスを持つ正規のホストに接続を提供するために、いくつかの回避策を実装できます。

オプション 1

ip arp inspection trustを使用して、ホストに接続されたインターフェイスを設定します。

```
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
```

オプション 2

ARPアクセスリストを使用して、スタティックホストを許可します。

```
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
```

オプション 3

静的ホストのバインディングテーブルエントリを設定します。

```
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
```

DAIで使用可能な追加オプション：

```
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-macの場合は、イーサネットヘッダーの送信元MACアドレスを、ARP本文の送信元MACアドレスと照合します。このチェックは、ARP要求とARP応答の両方に対して実行されます。有効にすると、異なるMACアドレスを持つパケットは無効として分類され、ドロップされます

dst-macの場合は、イーサネットヘッダー内の宛先MACアドレスを、ARP本文内のターゲットMACアドレスと照合します。このチェックは、ARP応答に対して実行されます。有効にすると、異なるMACアドレスを持つパケットは無効として分類され、ドロップされます。

IPの場合は、ARP本文で無効なIPアドレスや予期しないIPアドレスを確認します。アドレスには、0.0.0.0、255.255.255.255、およびすべてのIPマルチキャストアドレスが含まれます。送信元IPアドレスはすべてのARP要求と応答でチェックされ、ターゲットIPアドレスはARP応答でのみチェックされます。

ARPレート制限を設定することもできます。デフォルトでは、信頼できないインターフェイス上のARPトラフィックには15 ppsの制限があります。

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

IP ソース ガード

- IPSGは、非ルーテッドレイヤ2インターフェイス上のIPトラフィックを制限するために、DHCPスヌーピングバインディングデータベースと手動で設定されたIPソースバインディングに基づいてトラフィックをフィルタリングするセキュリティ機能です。

- ホストがネイバーのIPアドレスを使用しようとする場合は、IPSGを使用してトラフィック攻撃を防止できます。

- 信頼できないインターフェイスでDHCPスヌーピングが有効になっている場合は、IPSGを有効にできます。インターフェイスでIPSGを有効にすると、DHCPスヌーピングによって許可されるDHCPパケットを除き、そのインターフェイスで受信されるすべてのIPトラフィックがスイッチによってブロックされます。

- スイッチは、ハードウェアの送信元IPルックアップテーブルを使用して、IPアドレスをポートにバインドします。IPおよびMACフィルタリングでは、送信元IPと送信元MACルックアップを組み合わせて使用します。バインディングテーブル内の送信元IPアドレスを持つIPトラフィックは許可され、他のすべてのトラフィックは拒否されます。

- IP ソース バインディング テーブルには、DHCP スヌーピングにより学習されたバインディング、または手動で設定されたバインディング (スタティック IP ソース バインディング) があります。このテーブルのエントリには、IP アドレス、それに関連付けられた MAC アドレス、およびそれに関連付けられた VLAN 番号が含まれます。スイッチがIPソースバインディングテーブルを使用するのは、IPソースガードが有効な場合だけです。

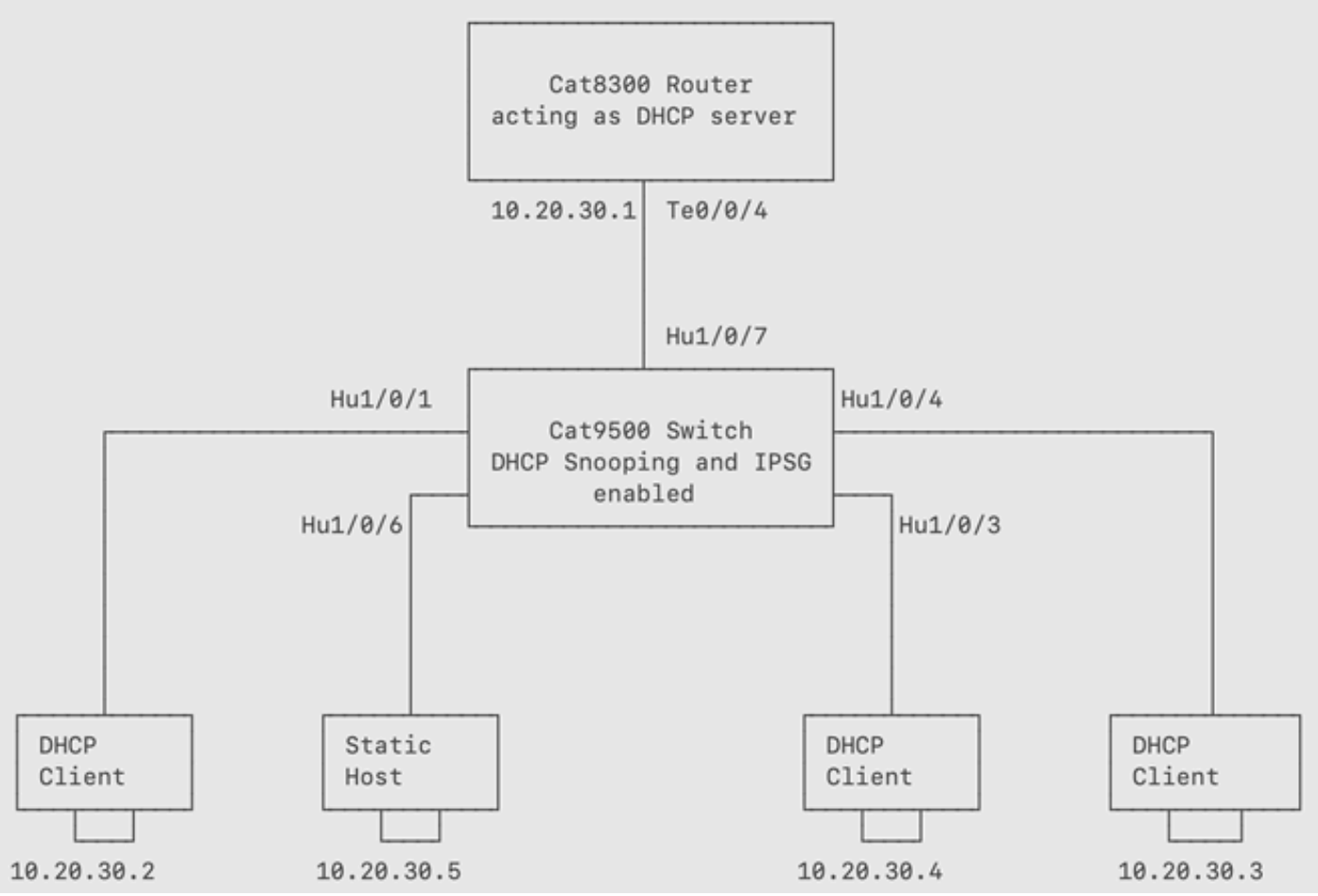
- 送信元IPアドレスフィルタリング、または送信元IPおよびMACアドレスフィルタリングを使用して、IPSGを設定できます。

スタティックホスト用のIPSG

- スタティックホスト用のIPSGを使用すると、DHCPを使用せずにIPSGを動作させることができます。スタティックホストのIPSGは、IPデバイストラッキングテーブルエントリを使用してポートACLをインストールします。スイッチは、ARP要求または他のIPパケットに基づいてスタティックエントリを作成し、特定のポートの有効なホストのリストを維持します。

参考資料

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スイッチは4つのホストに接続され、そのうち3つのホストはDHCPクライアントで、1つのホストには固定IPアドレスが割り当てられています。DHCPサーバは、DHCPプールを使用して設定されたCat8300シリーズルータです。
このトポロジを使用して、DHCPスヌーピングバインディングデータベースにMAC-IPバインディングが存在しないホストからのトラフィックをIPSGがどのように検出してブロックするかを示すことができます。

設定例:

ステップ 1：Cat9500スイッチでDHCPスヌーピングをグローバルに設定します。

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

ステップ 2：DHCPサーバに接続されているインターフェイスTe1/0/7を信頼できるポートとして設定します。これにより、DHCPオファーはインターフェイスに入力し、続いてDHCPクライアントに到達できます。

```
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
```

ステップ 3：DHCPクライアントに接続されているポートを、VLAN 10を許可するアクセスポートとして設定します。

```
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
```

ステップ 4：DHCPクライアントがDHCPサーバからIPアドレスを受信しているかどうかを確認します。

```
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

ステップ 5：すべてのエンドホストに接続されているインターフェイスでIPSGを設定します（DHCPクライアントx 3および固定IPアドレスを持つホストx 1）。

```
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
```

検証：

```
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

この出力から、DHCPスヌーピングバインディングテーブルにこのインターフェイスに対応するMAC-IPバインディングがないため、IP Addressフィールドが Hu1/0/6に対してdeny-allに設定されていることがわかります。

手順 6：Static_Hostから、IPアドレス10.20.30.2、10.20.30.3、および10.20.30.4のDHCPクライアントにpingを実行してみます。

```
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
```

IPSGで使用できるその他のオプション

デフォルトでは、IPSGはIPアドレスのみに基づいて、信頼できないポートの着信トラフィックをフィルタリングします。
IPアドレスとMACアドレスの両方に基づいてフィルタリングを実行する場合は、次の手順を実行します。

```
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
```

この出力では、フィルタタイプがip-macであることを確認できます。そのため、スイッチは送信元IPとMACアドレスの両方に基づいて、これらのインターフェイスの着信パケットをフィルタリングします。

DAIおよびIPSGのトラブルシューティングのヒント

- DAI

およびIPSG関連の問題をトラブルシューティングする際に最初に確認するのは、DHCPスヌーピングバインディングテーブルにデータが正しく取り込まれているかどうかを確認することです。

- これらの機能を有効にする前に、固定IPアドレスを持つエンドポイントを処理します。これらのデバイスの到達可能性を失いたくない場合は、スタティックバインディングを設定するか、前述の方法のいずれかを使用して、スイッチがこれらのエンドポイントを信頼するようにします。

- DHCPスヌーピングがまだ有効ではなく、クライアントがすでにDHCPサーバからIPを受信している環境でDAIまたはIPSGを設定する場合は、まずDHCPスヌーピングを有効にして、次の2つの手順のいずれかを実行します。

  - クライアント接続インターフェイスをバウンスして、リースを更新します。

  - クライアントがリースを自動的に更新するまで待ちます。これには時間がかかりますが、すべてのクライアント接続ポートを手動でバウンスする手間が省けます。

- 上記の2つの手順のいずれかを実行すると、新しいDORAトランザクションがトリガーされます。スイッチはDORAパケットをスニッフィングし、バインディングテーブルを更新します。これを行っておらず、DHCPスヌーピングの設定後にDAIまたはIPSGがすぐに有効になる場合、ネットワーク内のすべてのDHCPクライアントがネットワークへの接続を失うという問題が発生する可能性があります。

- DAIまたはIPSGが設定されている環境で接続の問題をトラブルシューティングする場合は、DHCPスヌーピングバインディングテーブルが破損していないことを確認します。スイッチがこのテーブルが格納されているデータ構造にアクセスできることを確認します。

- バインディングテーブルがメディアにエクスポートされる場合があり、スイッチのブート後に初期化に時間がかかったり、何らかの理由でスイッチからアクセスできなくなったりすることがあります。このようなシナリオでは、接続上の問題が発生する可能性があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。