Identificar e Solucionar Problemas de Inspeção ARP Dinâmica (DAI - Dynamic ARP Inspection) e Proteção de Origem IP (IPSG - IP Source Guard) em Switches Catalyst

Contents

Introdução

Este documento descreve como a Inspeção ARP Dinâmica (DAI - Dynamic ARP Inspection) e a Proteção de Origem IP (IPSG - IP Source Guard) funcionam e como validá-las nos Switches Catalyst 9K.

Rastreamento de DHCP e recursos relacionados

Antes de mergulhar no DAI e no IPSG, você precisa discutir rapidamente sobre o DHCP Snooping, que é um pré-requisito para o DAI e o IPSG.

O DHCP (Dynamic Host Configuration Protocol) é um protocolo cliente/servidor que fornece automaticamente um host IP (Internet Protocol) com seu endereço IP e outras informações de configuração relacionadas, como a máscara de sub-rede e o gateway padrão. Os RFCs 2131 e 2132 definem o DHCP como um padrão da Internet Engineering Task Force (IETF) baseado no Protocolo de Bootstrap (BOOTP), um protocolo com o qual o DHCP compartilha muitos detalhes de implementação. O DHCP permite que os hosts obtenham as informações de configuração TCP/IP necessárias de um servidor DHCP.

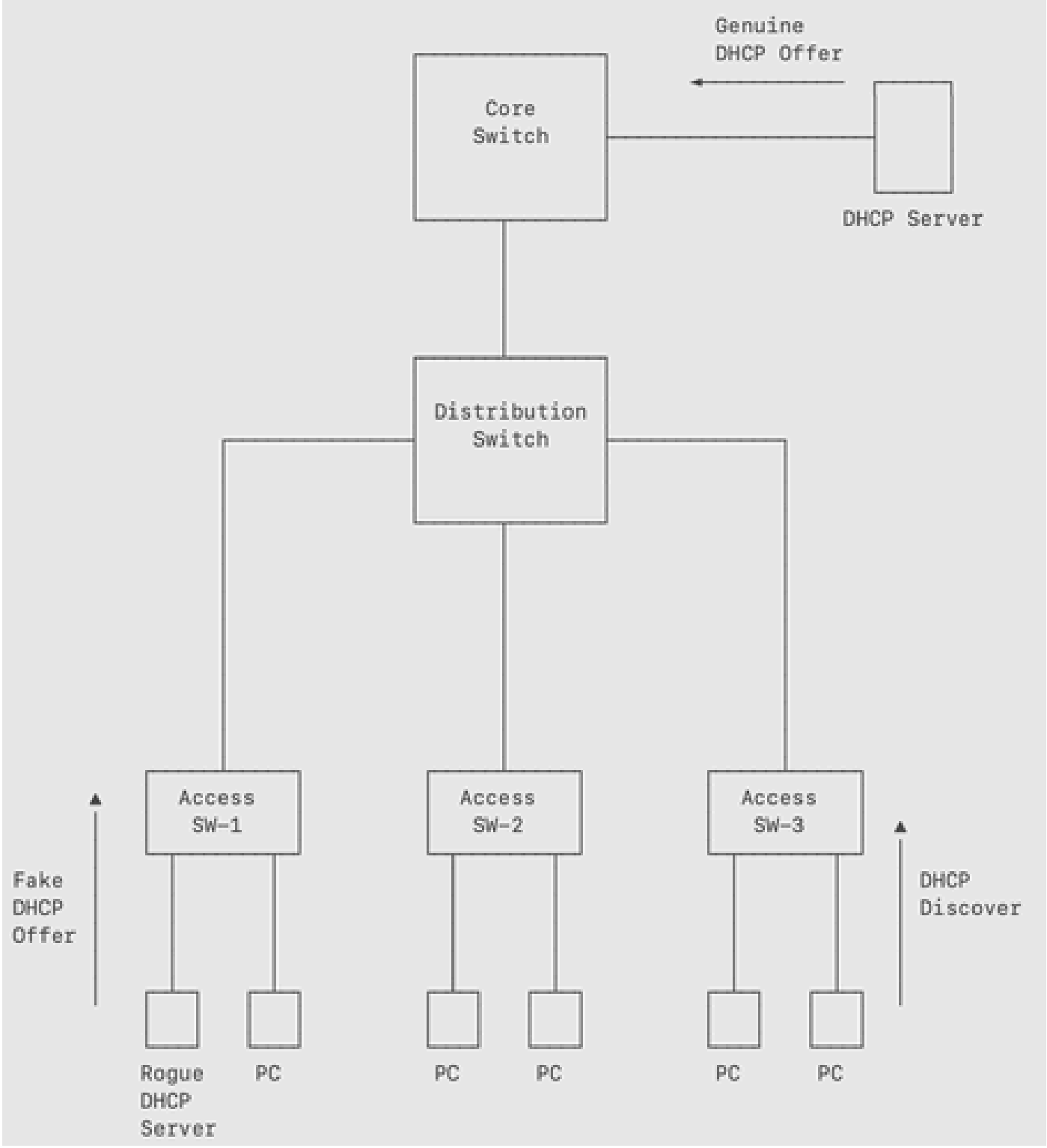
O rastreamento de DHCP é um recurso de segurança que funciona como um firewall entre hosts não confiáveis e servidores DHCP confiáveis. O recurso de rastreamento de DHCP executa estas atividades:

- Valida as mensagens DHCP recebidas de fontes não confiáveis e filtra as mensagens inválidas.
- Limita a taxa de tráfego DHCP de fontes confiáveis e não confiáveis.
- Cria e mantém o banco de dados de associação de rastreamento de DHCP, que contém informações sobre hosts não confiáveis com endereços IP alugados.
- Utiliza o banco de dados de associação de rastreamento de DHCP para validar solicitações subsequentes de hosts não confiáveis.

O DAI é um recurso de segurança que valida pacotes ARP (Address Resolution Protocol) em uma rede. O DAI permite que um administrador de rede intercepte, registre e descarte pacotes ARP com endereços MAC inválidos para vinculações de endereço IP. Esse recurso protege a rede de certos ataques "man-in-the-middle".

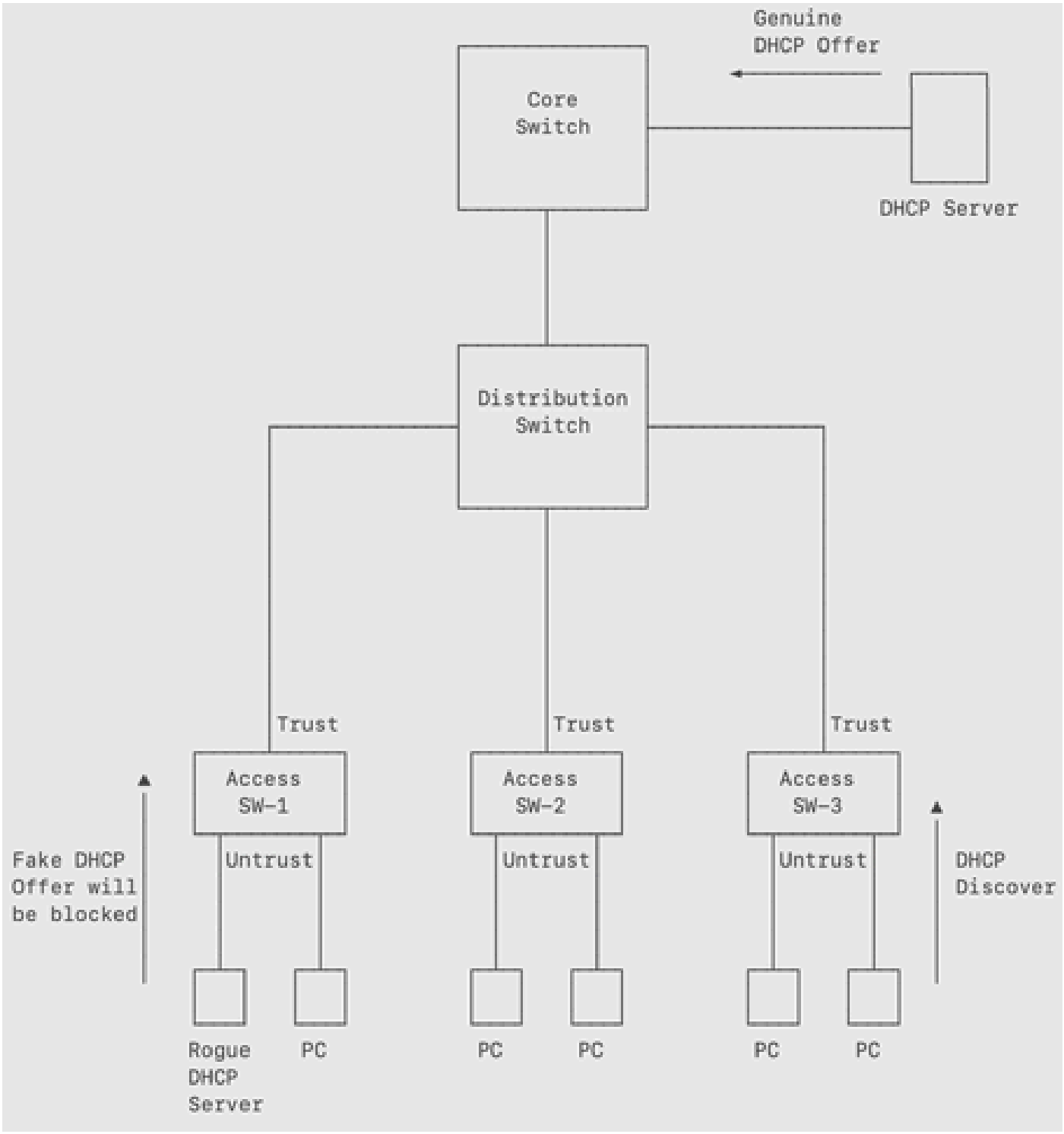
O IPSG é um recurso de segurança que restringe o tráfego IP em interfaces de Camada 2 não roteadas, filtrando o tráfego com base no banco de dados de associação de rastreamento de DHCP e em associações de origem de IP configuradas manualmente. Você pode usar o IPSG para evitar ataques de tráfego se um host tentar usar o endereço IP de seu vizinho.

Cenário sem rastreamento de DHCP



1. Neste diagrama, você pode ver que vários clientes gostariam de receber um endereço IP do servidor DHCP que está conectado ao switch central.
2. No entanto, há um servidor DHCP mal-intencionado/invasor que está conectado a um dos switches da camada de acesso que podem receber as descobertas de DHCP e enviar as ofertas de DHCP mais rápido do que o servidor DHCP real.
3. O invasor pode definir o endereço de gateway na mensagem de oferta de forma que ele possa receber todo o tráfego do cliente, comprometendo assim a confidencialidade da comunicação.
4. Isso é conhecido como o ataque do Homem no Meio.

Cenário com rastreamento de DHCP

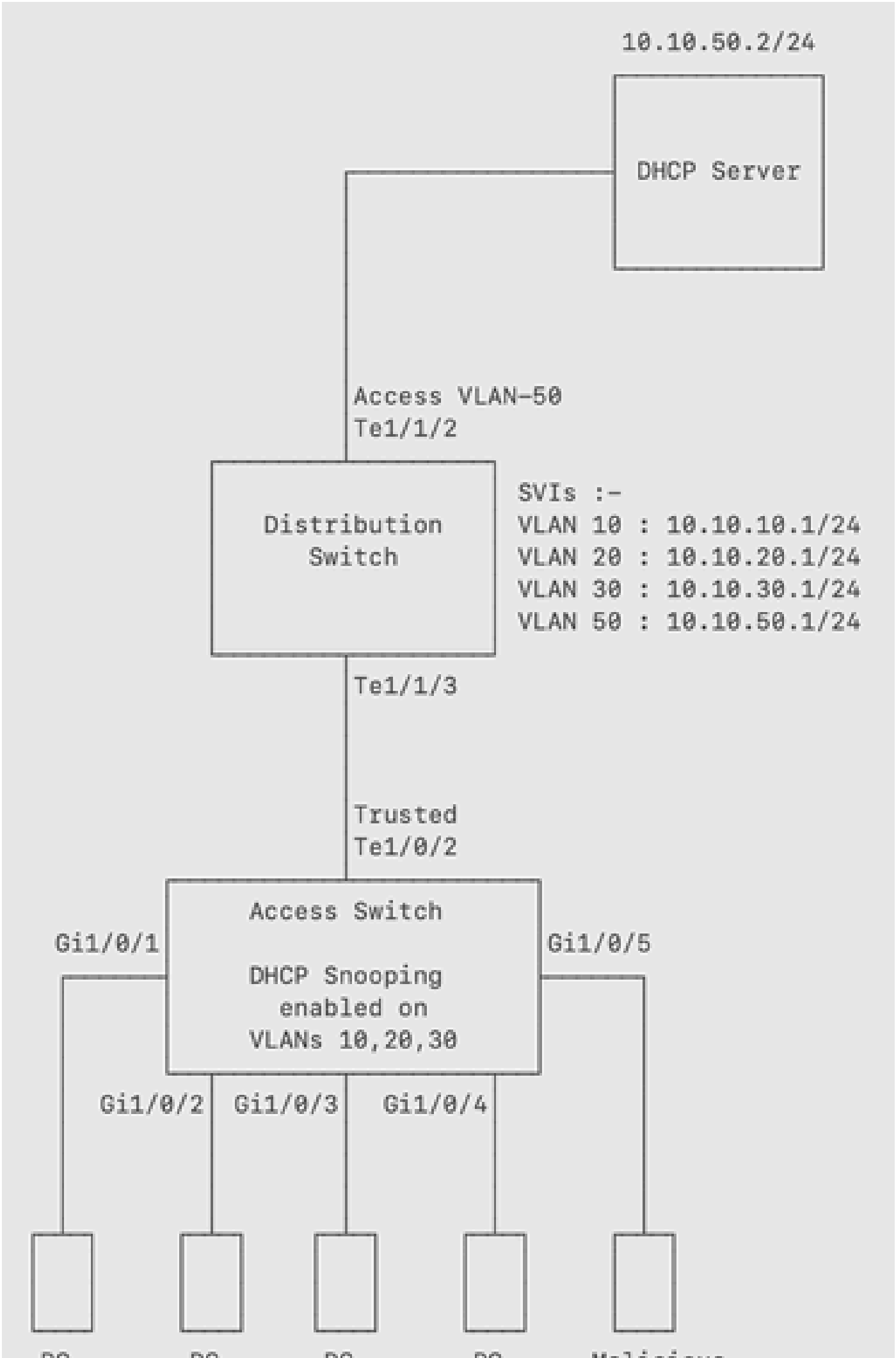


1. Ao habilitar o rastreamento de DHCP nos Switches de Acesso, configure o switch para escutar o tráfego DHCP e parar qualquer pacote DHCP mal-intencionado recebido em portas não confiáveis.
2. Assim que você ativar o rastreamento de DHCP no Switch, todas as interfaces se tornarão automaticamente não confiáveis.
3. Mantenha as portas conectadas aos dispositivos finais não confiáveis e configure as portas conectadas ao servidor DHCP original como confiáveis.
4. Uma interface não confiável bloqueará mensagens de oferta DHCP. As mensagens de oferta

DHCP só serão permitidas em portas confiáveis.
5. Você pode limitar o número de pacotes de descoberta DHCP que os hosts finais podem enviar a uma interface não confiável por segundo. Esse é um mecanismo de segurança para proteger o servidor DHCP de um número anormalmente alto de descobertas de DHCP de entrada que podem esgotar o pool em pouco tempo.

Nesta seção, é explicado como configurar o DHCP Snooping em uma rede comutada:

Topologia:


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
```

Etapa 2. Configure a confiança de rastreamento de DHCP em todas as interfaces do Switch de acesso que recebem ofertas de DHCP de servidores DHCP genuínos. O número dessas interfaces depende do projeto de rede e do posicionamento dos servidores DHCP. Essas são as interfaces que estão indo em direção ao Servidor DHCP genuíno.

Switch de acesso:

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

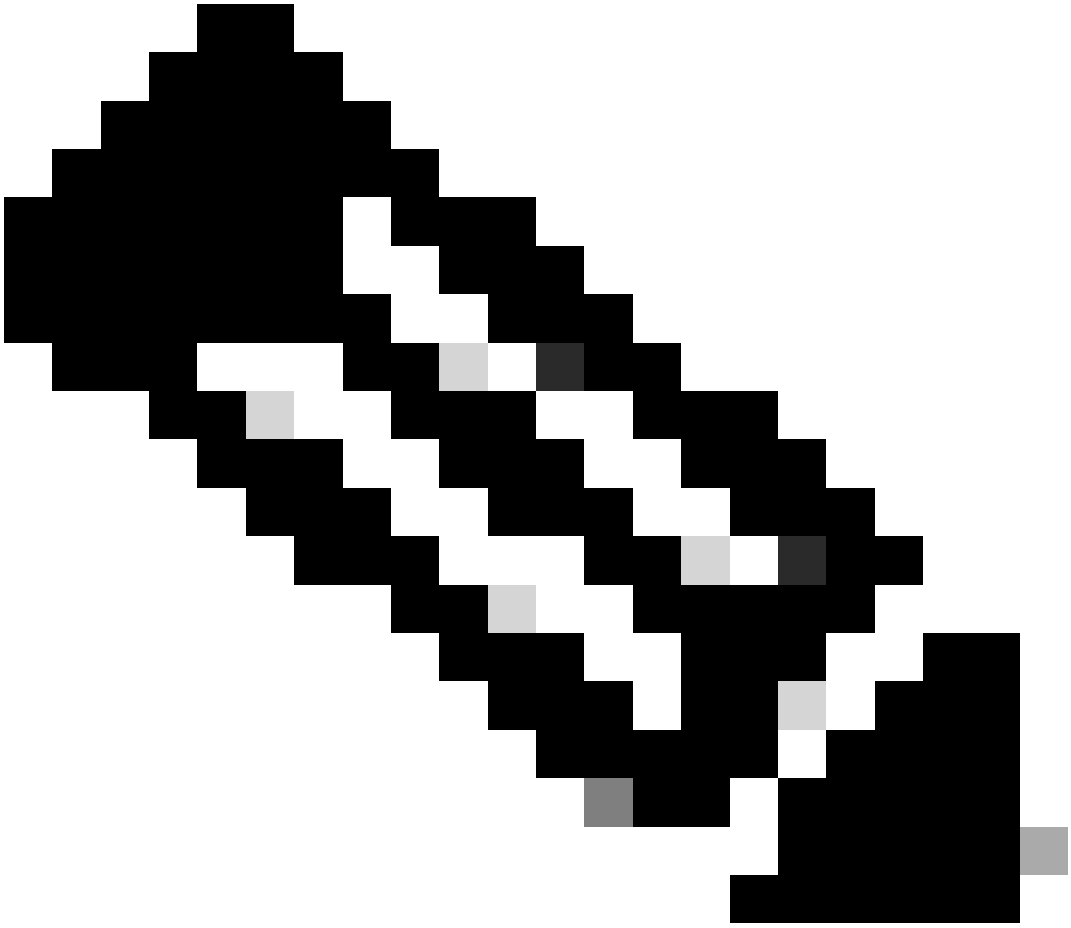
Etapa 3. Depois que você configurar o rastreamento de DHCP globalmente, todas as portas no Switch se tornarão não confiáveis automaticamente (exceto aquelas em que você confia manualmente, como mostrado anteriormente). No entanto, você pode configurar o número de pacotes de descoberta DHCP que os hosts finais podem enviar a interfaces não confiáveis por segundo.
Esse é um mecanismo de segurança para proteger o servidor DHCP de um número anormalmente alto de descobertas de DHCP de entrada que podem esgotar o pool em pouco tempo.

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

Verificação:

```
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:
```



Observação: se você observar essa saída, verá que a Gi1/0/5 conectada ao servidor DHCP mal-intencionado é mencionada na **show ip dhcp snooping** saída como não confiável.

Assim, o DHCP Snooping fará todas as verificações nessas portas.

Por exemplo, isso fará com que todas as ofertas de DHCP de entrada nessa porta (Gi1/0/5) sejam descartadas.

Esta é a tabela de ligação de rastreamento de DHCP, mostrando o endereço IP, o endereço MAC e a interface para 3 clientes em 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

Para fins de demonstração, ip dhcp snooping trust a configuração é removida de em Te1/0/2 no Switch de acesso. Examine os logs gerados no Switch:

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

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

Total cdp entries displayed : 1
```

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

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

*Apr 4 01:12:47.149: %DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on 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
```

- Como você pode ver, o Switch de acesso está descartando os pacotes de oferta de DHCP recebidos em Te1/0/2, já que não é mais confiável.

- Os endereços MAC nos registros pertencem às SVIs das VLANs 10,20 e 30, pois são eles que estão enviando essas ofertas do servidor DHCP para esses clientes.

Envenenamento ARP

O ARP fornece comunicação IP dentro de um domínio de broadcast de Camada 2 mapeando um endereço IP para um endereço MAC. É um protocolo simples, mas vulnerável a um ataque chamado envenenamento ARP.

A inviabilização ARP é um ataque em que um invasor envia um pacote de resposta ARP falso na rede.

Um usuário mal-intencionado pode atacar hosts, switches e roteadores conectados à sua rede de Camada 2, envenenando os caches ARP de

sistemas conectados à sub-rede e interceptando o tráfego destinado a outros hosts na sub-rede

Este é o clássico ataque do Homem no meio.

Mecanismos de prevenção

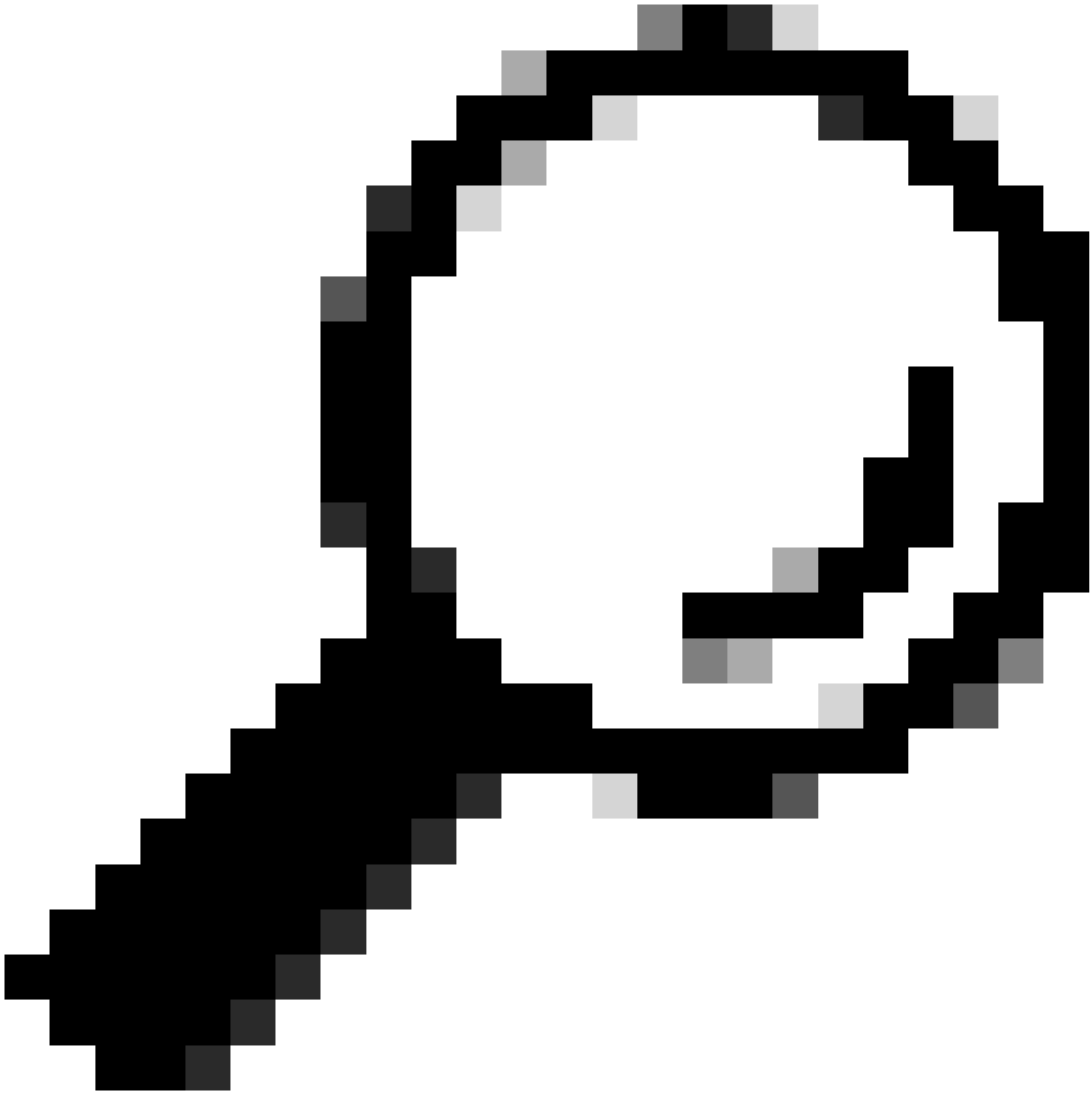
Inspeção ARP dinâmica (DAI)

A inspeção ARP dinâmica é um recurso de segurança que valida os pacotes ARP em uma rede. Ele intercepta, registra e descarta pacotes ARP com associações inválidas de endereço IP para MAC. Esse recurso protege a rede de certos ataques de intermediários.

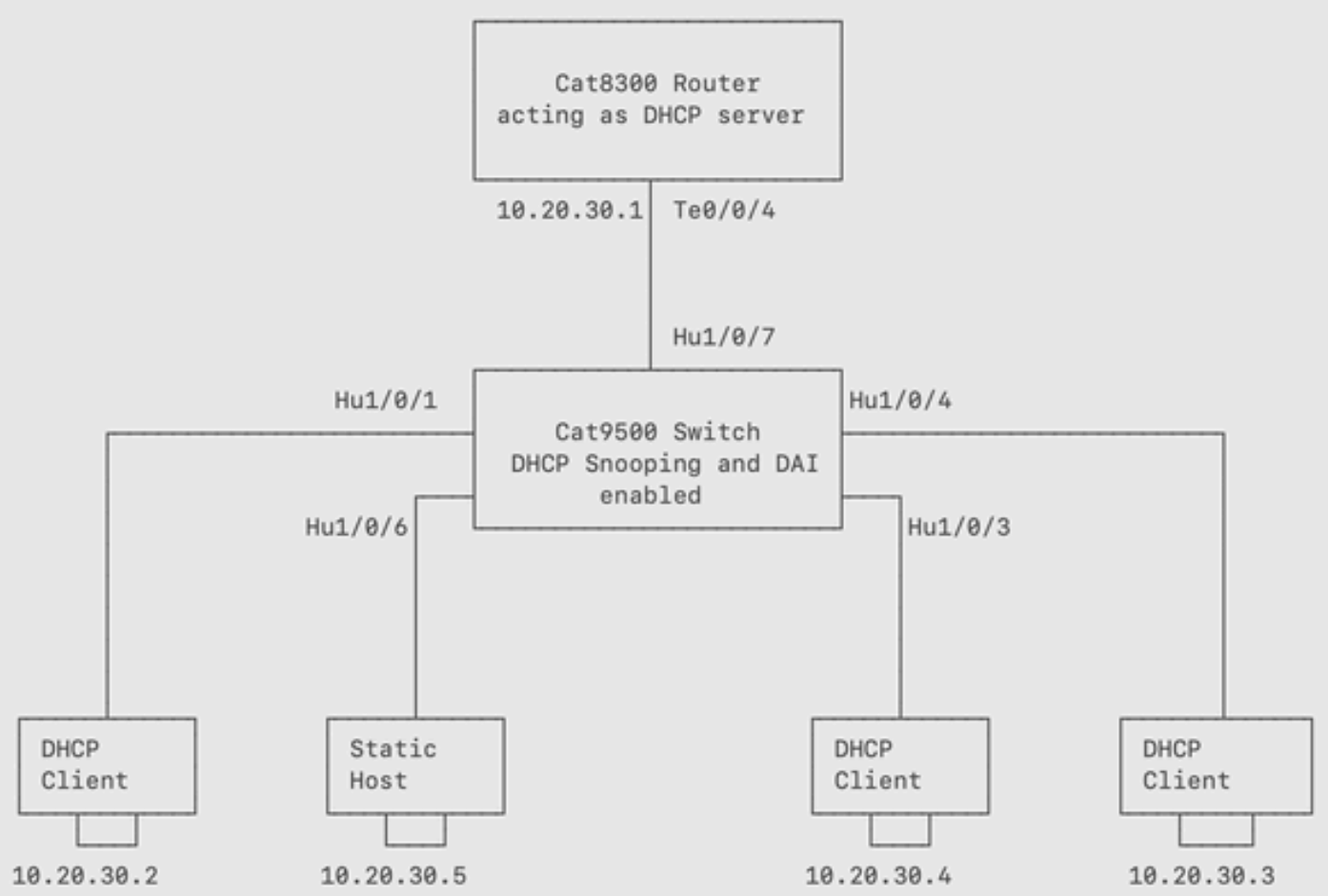
A inspeção ARP dinâmica garante que somente as solicitações e respostas ARP válidas sejam retransmitidas. O switch executa estas atividades:

- Intercepta todas as solicitações e respostas ARP em portas não confiáveis
- Verifica se cada um desses pacotes interceptados tem uma associação válida de endereço IP para MAC antes de atualizar o cache ARP local ou antes de encaminhar o pacote para o destino apropriado
- Descarta pacotes ARP inválidos

A inspeção ARP dinâmica determina a validade de um pacote ARP com base em associações válidas de endereço IP para MAC armazenadas em um banco de dados confiável, o banco de dados de associação de rastreamento DHCP.
Esse banco de dados é criado pelo rastreamento de DHCP se o rastreamento de DHCP estiver habilitado nas VLANs e no switch. Se o pacote ARP for recebido em uma interface confiável, o switch encaminhará o pacote sem nenhuma verificação.
Em interfaces não confiáveis, o switch encaminha o pacote somente se ele for válido.



Dica: consulte 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



Esta imagem demonstra o Switch Cat9500 conectado a quatro hosts, dos quais 3 hosts são clientes DHCP e 1 host tem endereço IP estático (10.20.30.5). O servidor DHCP é um roteador da série Cat8300 configurado com um pool DHCP.

A topologia acima é usada para demonstrar como o DAI detecta solicitações ARP inválidas em uma interface e protege a rede de invasores mal-intencionados.

Configuração:

Etapa 1. Configure globalmente o rastreamento de DHCP e o DAI no 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
```

Etapa 2. Configure a interface Hu1/0/7 que está conectada ao servidor DHCP como uma porta confiável. Isso permitirá que as ofertas DHCP ingressem na interface e, subsequentemente, acessem os clientes 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
```

Etapa 3. Configure as portas conectadas aos clientes DHCP como portas de acesso que permitem a 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
```

Etapa 4. Verifique se os clientes DHCP receberam o endereço IP do servidor DHCP a partir da tabela de ligação de rastreamento de DHCP no Switch 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
```

Você também pode verificar as vinculações no servidor 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

Etapa 5: Altere o endereço IP do host conectado a Hu1/0/6 de 10.20.30.5 para 10.20.30.2 e tente fazer ping nos outros clientes DHCP desse host.

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

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

Esses logs ARP inválidos podem ser vistos no Switch 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
```

- Como você pode ver, ao tentar fazer ping em 10.20.30.3 e 10.20.30.4 a partir de Static_Host, você não pode fazer isso. Embora Static_Host tenha tentado falsificar o endereço IP do cliente DHCP legítimo, ele não pôde fazer isso porque qualquer pacote ARP que chega em Hu1/0/6 será inspecionado pelo Switch e comparado com os dados presentes na tabela de ligação de rastreamento de DHCP.

- Os logs subsequentes do Switch Cat9500 confirmam que as solicitações ARP que estão sendo enviadas do Static_Host para os clientes DHCP estão sendo eliminadas.

- O Switch Cat9500 faz isso consultando o banco de dados de associação de rastreamento de DHCP.

- Quando uma solicitação ARP ingressa Hu1/0/6 com o MAC-IP de origem que não corresponde aos valores presentes no banco de dados de associação de rastreamento de DHCP, o Switch descarta a solicitação ARP.

Etapa 6. Verificação:

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

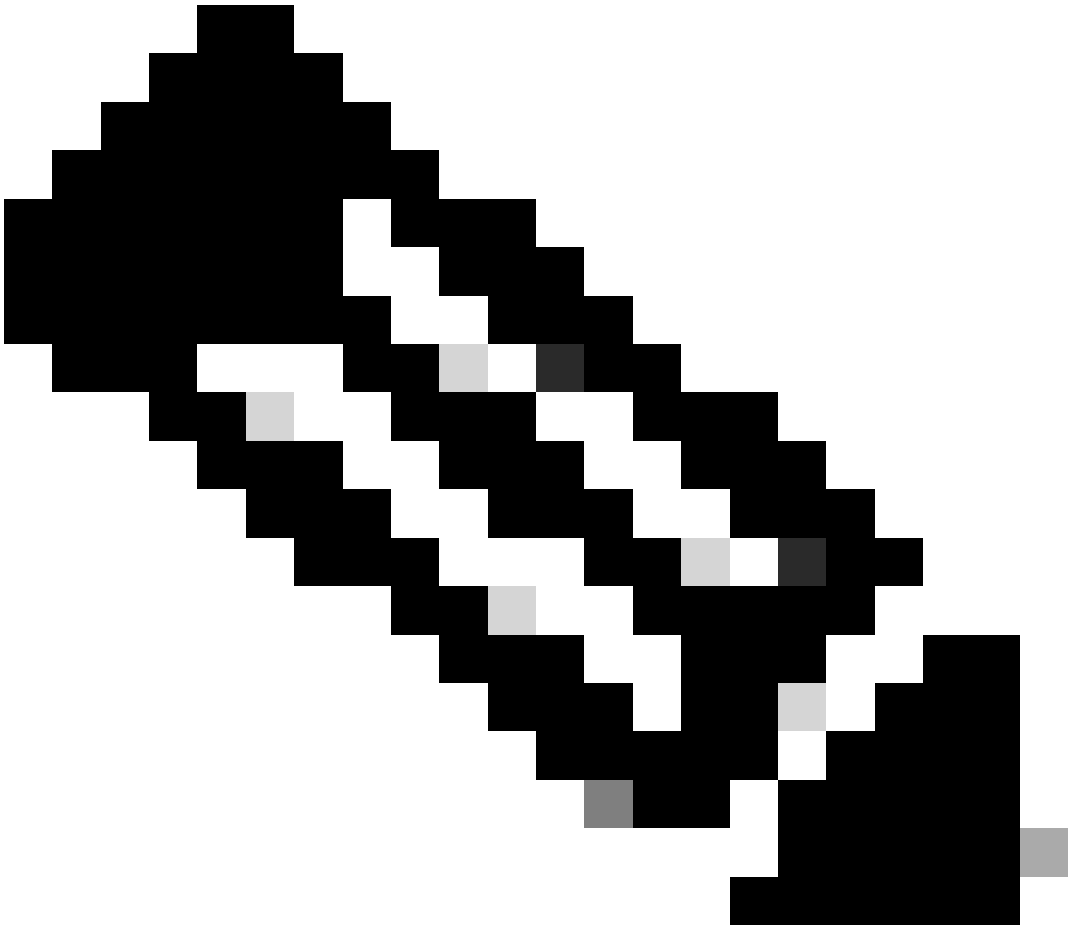
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
10	9	39	39	0

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

Nesta saída, você pode ver o número de pacotes descartados e permitidos pelo DAI na VLAN 10 no Switch Cat9500.



Observação: um cenário muito importante poderia ser um host legítimo na rede que tenha um endereço IP estático (por exemplo, 10.20.30.5) atribuído a ele?

Embora o host não esteja tentando falsificar nada, ele ainda estará isolado da rede porque seus dados de associação MAC-IP não estão presentes no banco de dados de associação de rastreamento de DHCP.

Isso ocorre porque o host estático nunca usou o DHCP para receber o endereço IP, já que ele foi atribuído estaticamente a ele.

Temos algumas soluções alternativas que podem ser implementadas para fornecer conectividade a hosts legítimos que tenham endereços IP estáticos.

Opção 1.

Configure a interface conectada ao host com 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
```

Opção 2.

Permita o host estático usando uma lista de acesso 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
```

Opção 3.

Configure uma entrada de tabela de ligação para o Host Estático.

```
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
```

Opções adicionais disponíveis com o 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
```

Para src-mac, verifique o endereço MAC origem no cabeçalho Ethernet em relação ao endereço MAC do remetente no corpo ARP. Essa verificação é executada nas solicitações e respostas ARP. Quando ativados, os pacotes com endereços MAC diferentes são classificados como inválidos e são descartados

Para dst-mac, verifique o endereço MAC destino no cabeçalho Ethernet em relação ao endereço MAC destino no corpo ARP. Essa verificação é executada para respostas ARP. Quando ativados, os pacotes com endereços MAC diferentes são classificados como inválidos e são descartados.

Para IP, verifique se há endereços IP inválidos e inesperados no corpo do ARP. Os endereços incluem 0.0.0.0, 255.255.255.255 e todos os endereços IP multicast. Os endereços IP do remetente são verificados em todas as solicitações e respostas ARP, e os endereços IP de destino são verificados somente nas respostas ARP.

Você também pode configurar a limitação de taxa ARP. Por padrão, há um limite de 15 pps para o tráfego ARP em interfaces não confiáveis:

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

Proteção de origem de IP

- O IPSG é um recurso de segurança que restringe o tráfego IP em interfaces de Camada 2 não roteadas, filtrando o tráfego com base no banco de dados de associação de rastreamento de DHCP e em associações de origem de IP configuradas manualmente.

- Você pode usar o IPSG para evitar ataques de tráfego se um host tentar usar o endereço IP de seu vizinho.

- Você pode habilitar o IPSG quando o rastreamento de DHCP está habilitado em uma interface não confiável. Depois que o IPSG é habilitado em uma interface, o switch bloqueia todo o tráfego IP recebido na interface, exceto os pacotes DHCP permitidos pelo rastreamento de DHCP.

- O switch usa uma tabela de pesquisa de IP de origem no hardware para vincular endereços IP a portas. Para filtragem de IP e MAC, é usada uma combinação de consultas de IP de origem e MAC de origem. O tráfego IP com um endereço IP de origem na tabela de vinculação é permitido, todos os outros tráfegos são negados.

- A tabela de associação de origem IP tem associações que são aprendidas pelo rastreamento de DHCP ou são configuradas manualmente (associações de origem IP estáticas). Uma entrada nesta tabela tem um endereço IP, seu endereço MAC associado e seu número de VLAN associado. O switch usa a tabela de vinculação de origem de IP somente quando a proteção de origem de IP está habilitada.

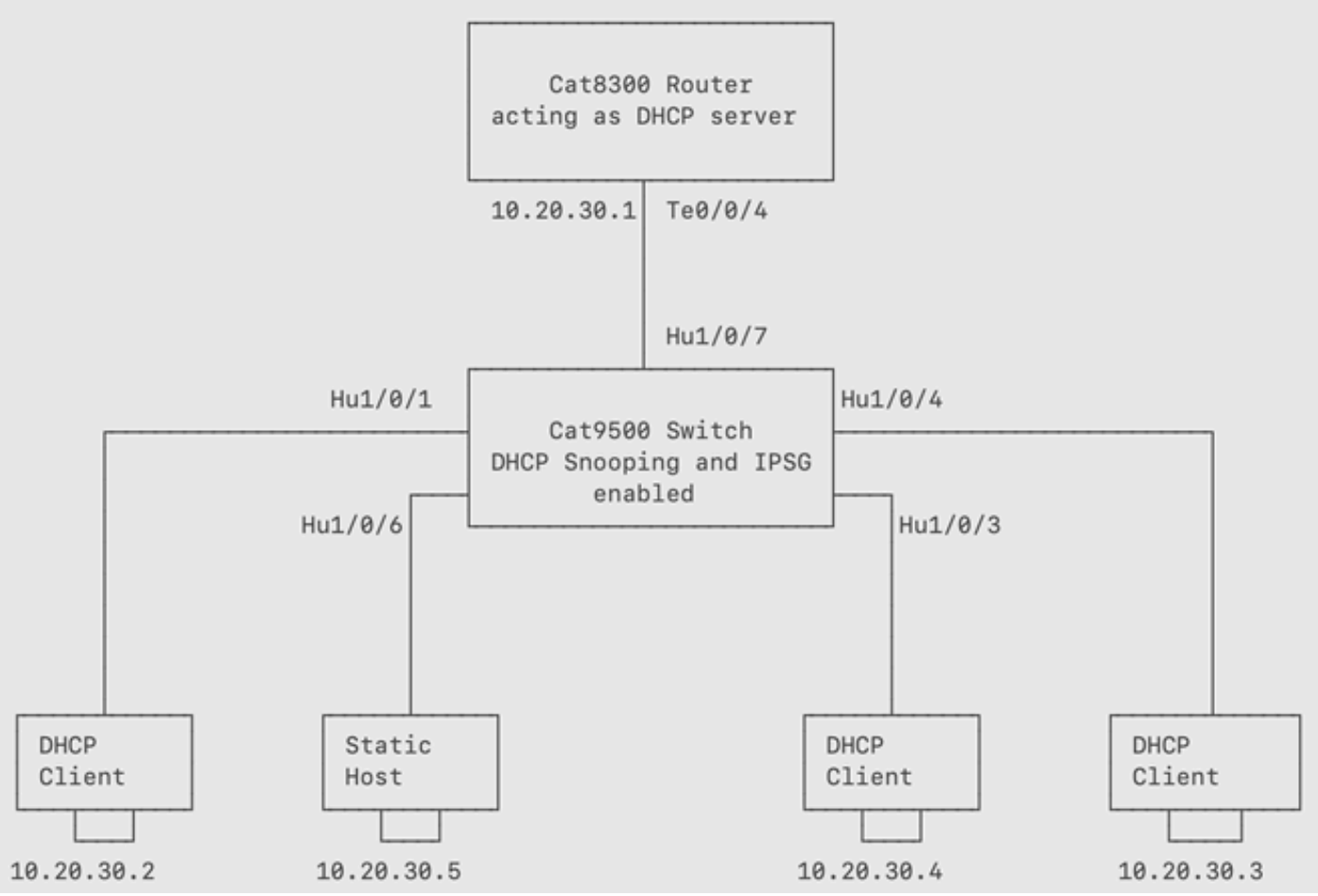
- Você pode configurar o IPSG com a filtragem de endereços IP de origem ou com a filtragem de endereços IP e MAC de origem.

IPSG para hosts estáticos

- O IPSG para hosts estáticos permite que o IPSG funcione sem DHCP. O IPSG para hosts estáticos depende das entradas da tabela de rastreamento do dispositivo IP para instalar ACLs de porta. O switch cria entradas estáticas com base em solicitações ARP ou outros pacotes IP para manter a lista de hosts válidos para uma determinada porta.

Referência:

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



O Switch Cat9500 está conectado a quatro hosts, dos quais 3 são clientes DHCP e 1 host tem um endereço IP estático. O servidor DHCP é um roteador da série Cat8300 configurado com um pool DHCP.
Você pode usar essa topologia para demonstrar como o IPSG detecta e bloqueia o tráfego de hosts cujas associações MAC-IP não estão presentes no banco de dados de associação de rastreamento de DHCP.

Configurar:

Etapa 1. Configure o rastreamento de DHCP globalmente no Switch Cat9500.

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

Etapa 2. Configure a interface Te1/0/7 que está conectada ao servidor DHCP como uma porta confiável. Isso permite que as ofertas DHCP ingressem na interface e acessem subsequentemente os clientes 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
```

Etapa 3. Configure as portas conectadas aos clientes DHCP como portas de acesso que permitem a 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
```

Etapa 4. Verifique se os clientes DHCP receberam o endereço IP do servidor 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

Etapa 5. Configure o IPSG nas interfaces conectadas a todos os hosts finais (3x clientes DHCP e 1x hosts com endereço IP estático).

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
```

Verificação:

```
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
```

Nessa saída, você pode ver que o campo Endereço IP está definido como deny-all para Hu1/0/6 porque não há nenhuma associação MAC-IP correspondente a essa interface na tabela de associação de rastreamento DHCP.

Etapa 6. Tente fazer ping nos clientes DHCP com os endereços IP 10.20.30.2, 10.20.30.3 e 10.20.30.4 a partir do 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
```

Opções adicionais disponíveis com o IPSG:

Por padrão, o IPSG filtra o tráfego de entrada em portas não confiáveis com base apenas nos endereços IP.

Para executar a filtragem com base nos endereços IP e MAC, execute estas etapas.

```
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
```

Nesta saída, você pode ver que o tipo de filtro é ip-mac. Assim, o Switch agora filtra os pacotes de entrada nessas interfaces com base no IP de origem e no endereço MAC.

Dicas de solução de problemas para DAI e IPSG

- A primeira coisa a verificar durante a solução de problemas relacionados ao DAI e ao IPSG é verificar se a tabela de associação de rastreamento de DHCP foi preenchida corretamente.

- Antes de habilitar esses recursos, manipule os endpoints com endereços IP estáticos. Se você não quiser que esses dispositivos percam o alcance, configure ligações estáticas ou empregue uma das metodologias mencionadas anteriormente para fazer com que o Switch confie nesses endpoints.

- Ao configurar o DAI ou o IPSG em um ambiente em que o rastreamento de DHCP ainda não esteja habilitado e os clientes já tenham recebido IPs do servidor DHCP, primeiro habilite o rastreamento de DHCP e execute uma das duas etapas a seguir:

  - Devolva as interfaces conectadas ao cliente para que elas renovem seu aluguel.

  - Aguarde até que os clientes renovem automaticamente o leasing. Isso pode levar mais tempo, mas evita o incômodo de saltar manualmente para todas as portas conectadas ao cliente.

- A execução de qualquer uma das duas etapas acima acionará uma nova transação DORA. O Switch farejará os pacotes DORA e atualizará a tabela de vinculação. Se isso não for feito e o DAI ou o IPSG forem imediatamente ativados após a configuração do rastreamento de DHCP, você poderá ter um problema em que todos os clientes DHCP na rede percam a conectividade com a rede.

- Ao solucionar problemas de conectividade em um ambiente onde DAI ou IPSG está configurado, verifique se a tabela de associação de rastreamento de DHCP não está corrompida. Certifique-se de que o Switch possa acessar a estrutura de dados onde essa tabela está armazenada.

- Pode haver instâncias em que a tabela de vinculação é exportada para uma mídia que leva tempo para ser inicializada depois que o switch é inicializado ou se torna inacessível para o switch devido a algum motivo. Você pode ter observado problemas de conectividade nesses cenários.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.