排除Catalyst交換機中的動態ARP檢測(DAI)和IP源防護(IPSG)故障

目錄

簡介

本文檔介紹動態ARP檢測(DAI)和IP源防護(IPSG)如何工作，以及如何在Catalyst 9K交換機中驗證它們。

DHCP監聽和相關功能

在深入瞭解DAI和IPSG之前，您需要簡要討論DHCP監聽，這是DAI和IPSG的前提條件。

動態主機設定通訊協定(DHCP)是一種使用者端/伺服器通訊協定，可自動為網際網路通訊協定(IP)主機提供其IP位址及其他相關設定資訊，例如子網路遮罩和預設閘道。RFC 2131和2132將DHCP定義為基於Bootstrap協定(BOOTP)的網際網路工程任務組(IETF)標準，BOOTP是DHCP共用許多實施細節的協定。DHCP允許主機從DHCP伺服器獲取所需的TCP/IP配置資訊。

DHCP監聽是一種安全功能，類似於不受信任的主機與受信任的DHCP伺服器之間的防火牆。
DHCP監聽功能執行以下活動：

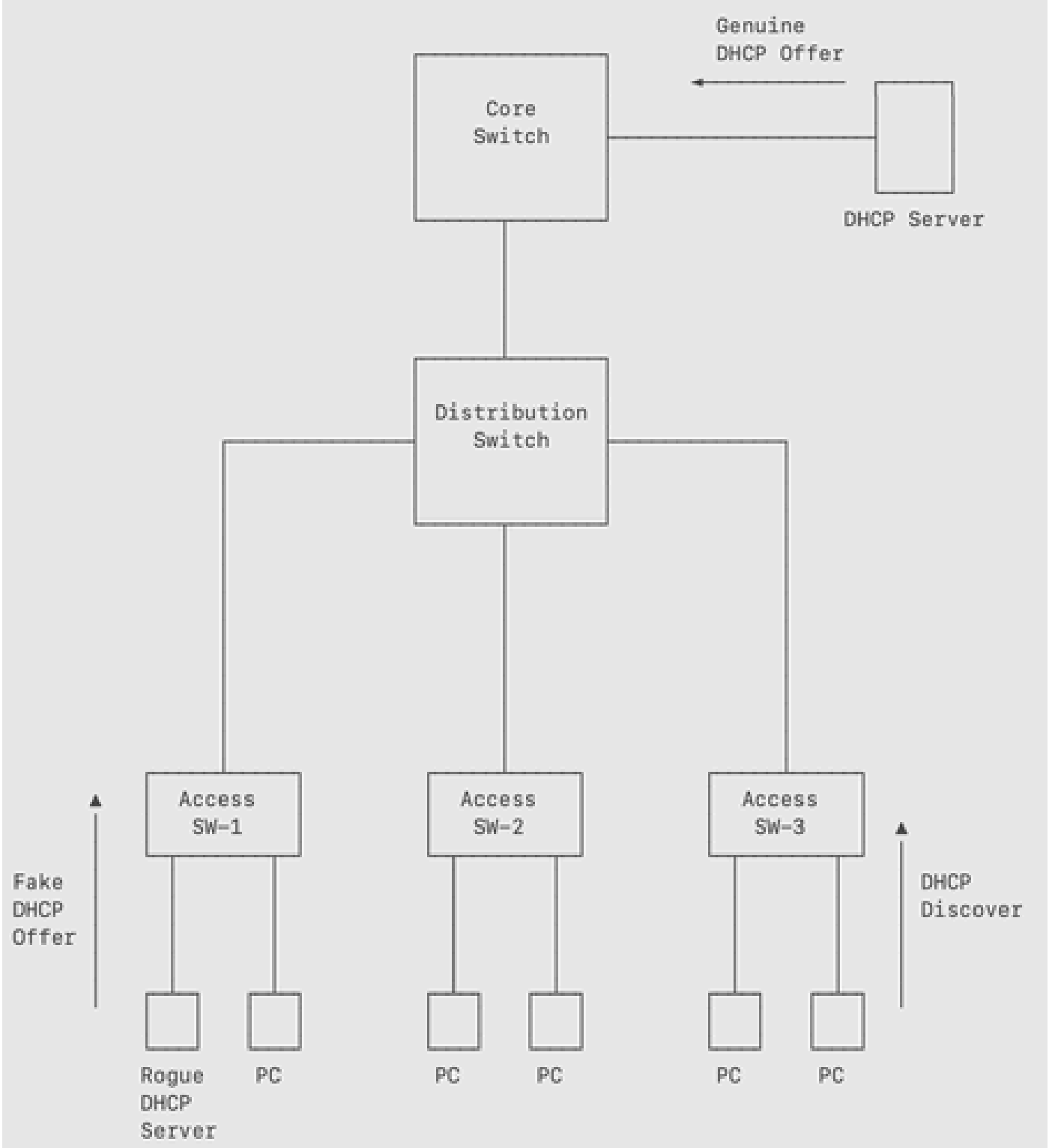
- 驗證從不受信任的來源接收的DHCP訊息，並篩選出無效的訊息。
- 對來自受信任和不受信任源的DHCP流量進行速率限制。
- 構建並維護DHCP監聽繫結資料庫，其中包含有關使用租用IP地址的不受信任主機的資訊。
- 使用DHCP監聽繫結資料庫驗證來自不受信任主機的後續請求。

DAI是一種安全功能，用於驗證網路中的地址解析協定(ARP)資料包。DAI允許網路管理員攔截、記錄和丟棄具有無效MAC地址到IP地址繫結的ARP資料包。此功能可保護網路免受某些「中間人」攻擊。

IPSG是一種安全功能，它透過根據DHCP監聽繫結資料庫和手動配置的IP源繫結過濾流量，來限制

非路由的第2層介面上的IP流量。如果主機嘗試使用其鄰居的IP地址，您可以使用IPSG來防止流量攻擊。

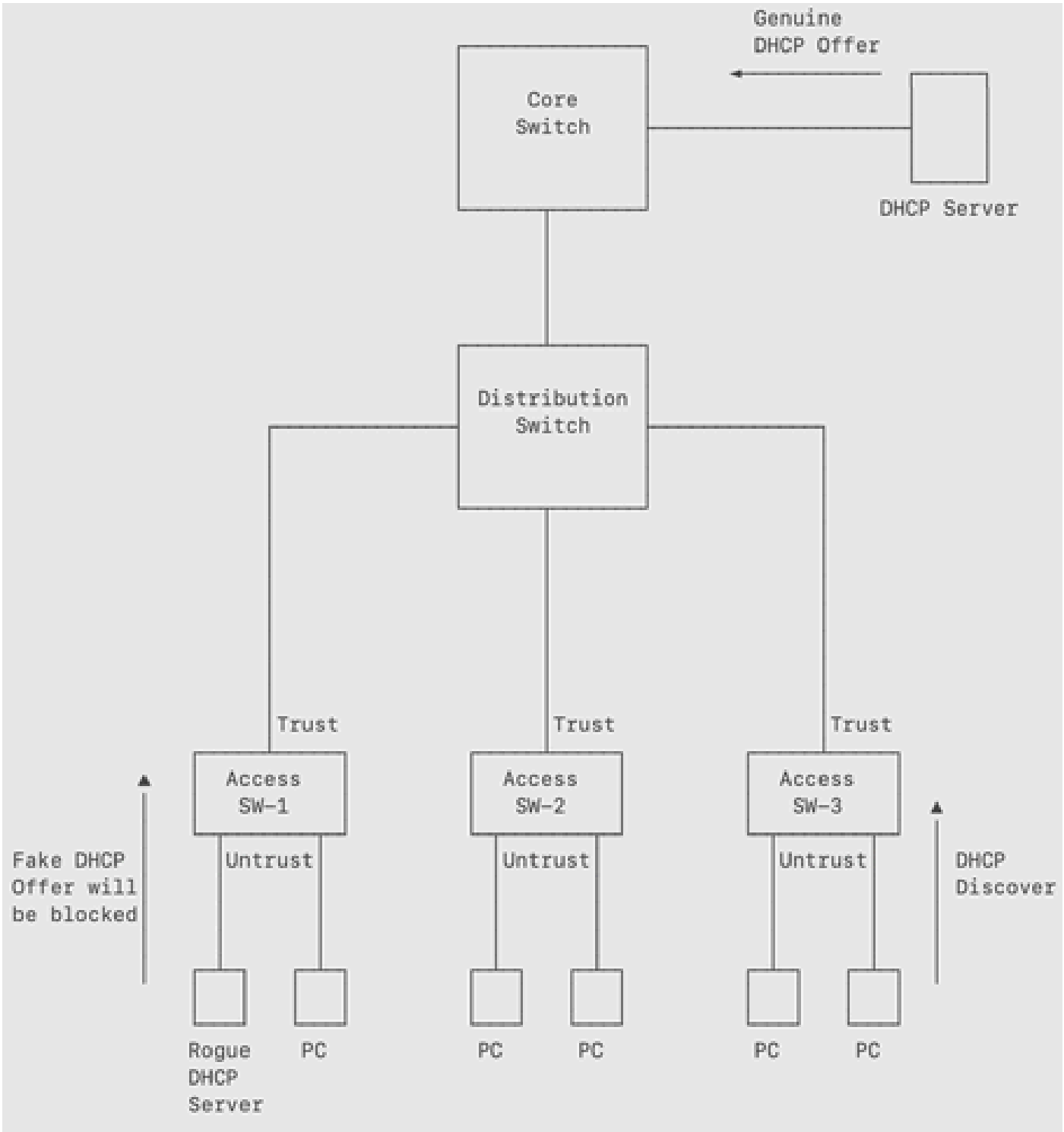
沒有DHCP監聽的案例



1. 在此圖中，您可以看到多個客戶端希望從連線到核心交換機的DHCP伺服器接收IP地址。
2. 但是，有一個惡意/惡意DHCP伺服器連線到接入層交換機之一，該伺服器可以接收DHCP發現並

傳送DHCP產品，其速度比實際DHCP伺服器更快。
3. 攻擊者可設定要約消息中的網關地址，使其能接收來自客戶端的所有流量，從而影響通訊的機密性。
4. 這被稱為「中間人」。

使用DHCP監聽的案例

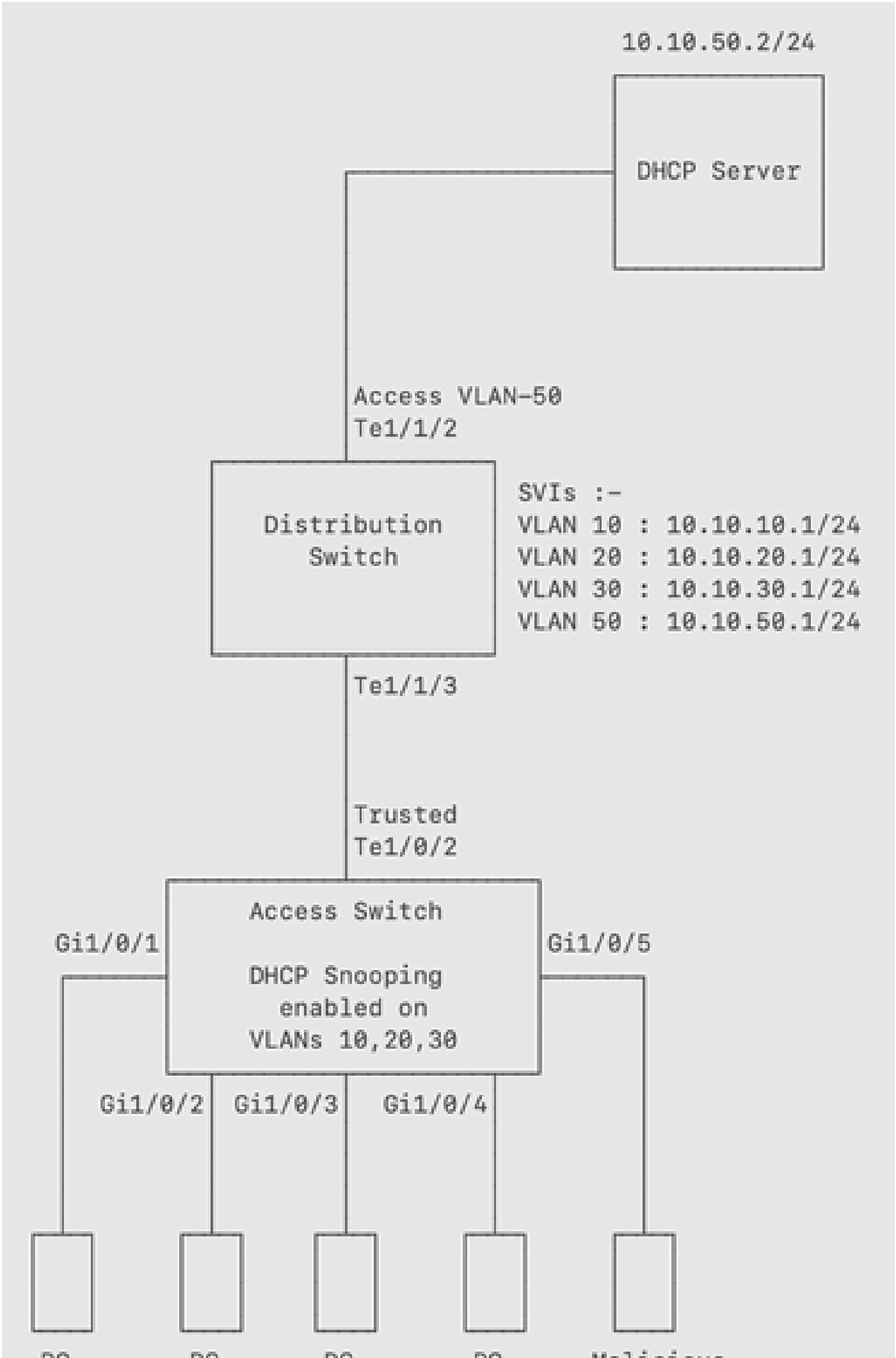


1. 透過在接入交換機中啟用DHCP監聽，將交換機配置為監聽DHCP流量，並停止在不可信埠上收到的任何惡意DHCP資料包。
2. 一旦在交換機中啟用DHCP監聽，所有介面就會自動變為不可信狀態。

3. 保持連線到終端裝置的埠不受信任，並將連線到正版DHCP伺服器的埠配置為受信任。
4. 不受信任的介面將阻止DHCP提供消息。DHCP offer消息只能在受信任的埠上使用。
5. 您可以限制終端主機每秒可傳送到不受信任介面的DHCP發現資料包的數量。 這是一種安全機制，可保護DHCP伺服器免受異常大量的傳入DHCP發現（這些發現可能很快耗盡池）的影響。

本節介紹如何在交換網路中配置DHCP監聽：

拓撲：


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
```

步驟 2.在接收正版DHCP伺服器提供的DHCP服務的接入交換機的所有介面上配置DHCP監聽信任。此類介面的數量取決於Network設計和DHCP伺服器的放置。這些介面將連線到正版DHCP伺服器。

接入交換機：

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

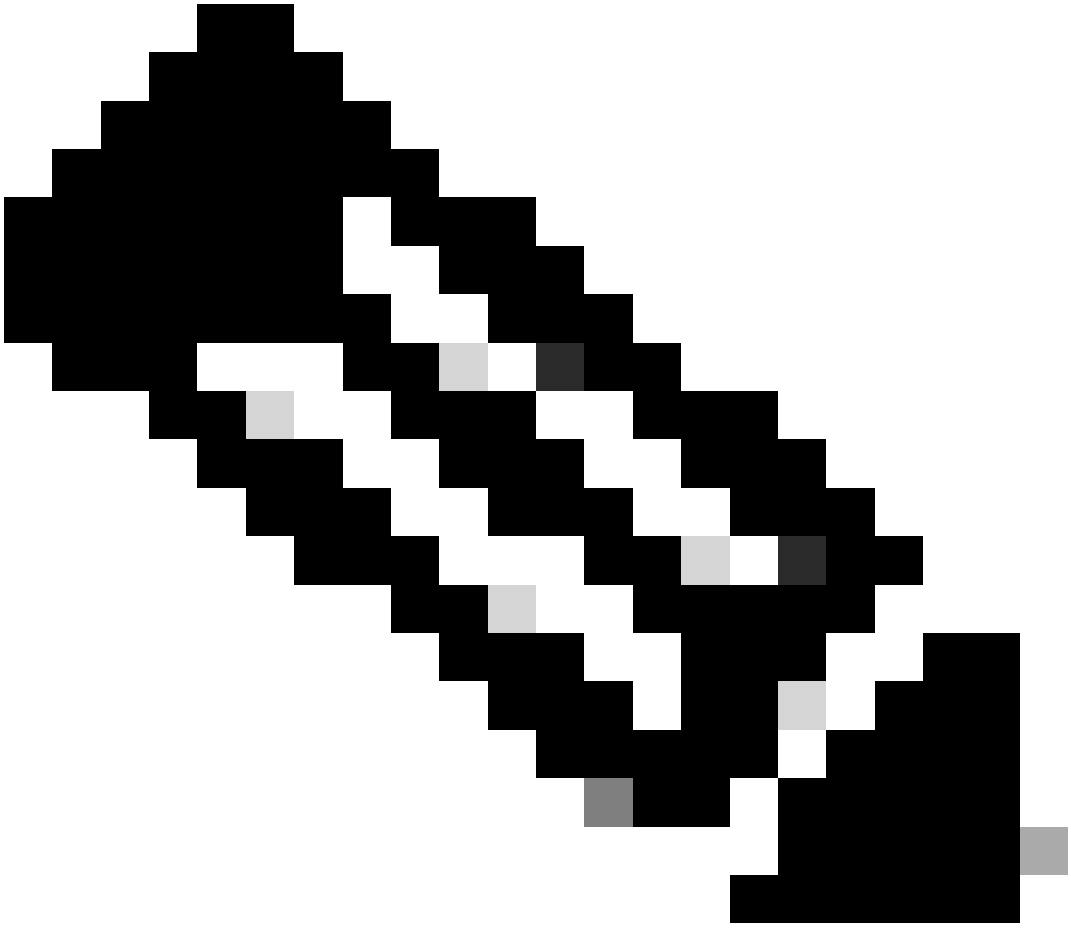
步驟 3.全局配置DHCP監聽後，交換機中的所有埠都會自動變為不可信狀態（手動信任埠除外，如前所示）。但是，您可以配置終端主機每秒可傳送到不受信任介面的DHCP發現資料包數。
這是一種安全機制，可保護DHCP伺服器免受異常大量的傳入DHCP發現（這些發現可能很快耗盡池）的影響。

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

驗證：

```
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:
```



注意：如果您檢視此輸出，則會看到連線到惡意DHCP伺服器的Gi1/0/5在**show ip dhcp snooping**輸出中被視為不受信任。

因此，DHCP監聽將對這些埠執行所有檢查。

例如，這將導致此埠(Gi1/0/5)上的所有傳入DHCP服務被丟棄。

以下是DHCP監聽繫結表，顯示Gi1/0/1、Gi1/0/2、Gi1/0/3上3個客戶端的IP地址、MAC地址和介面：

```
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
```

出於演示目的，ip dhcp snooping trust配置已從接入交換機的Te1/0/2下刪除。請檢視在Switch：路由器上

```
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
```

- 如您所見，接入交換機正在丟棄Te1/0/2上的傳入DHCP提供資料包，因為它不再受信任。
- 日誌中的MAC地址屬於VLAN 10、20和30的SVI，因為它們是從DHCP伺服器向這些客戶端傳送這些優惠資訊的客戶端。

ARP中毒

ARP透過將IP地址對映到MAC地址來提供第2層廣播域內的IP通訊。這是一個簡單的協定，但容易受到稱為ARP中毒的攻擊。

ARP毒化是一種攻擊，攻擊者在網路上傳送虛假的ARP應答資料包。

惡意使用者可以透過毒化連線到子網的系統的ARP快取並攔截流向子網中其他主機的流量來攻擊連線到第2層網路的主機、交換機和路由器

這是典型的中間人攻擊。

預防機制

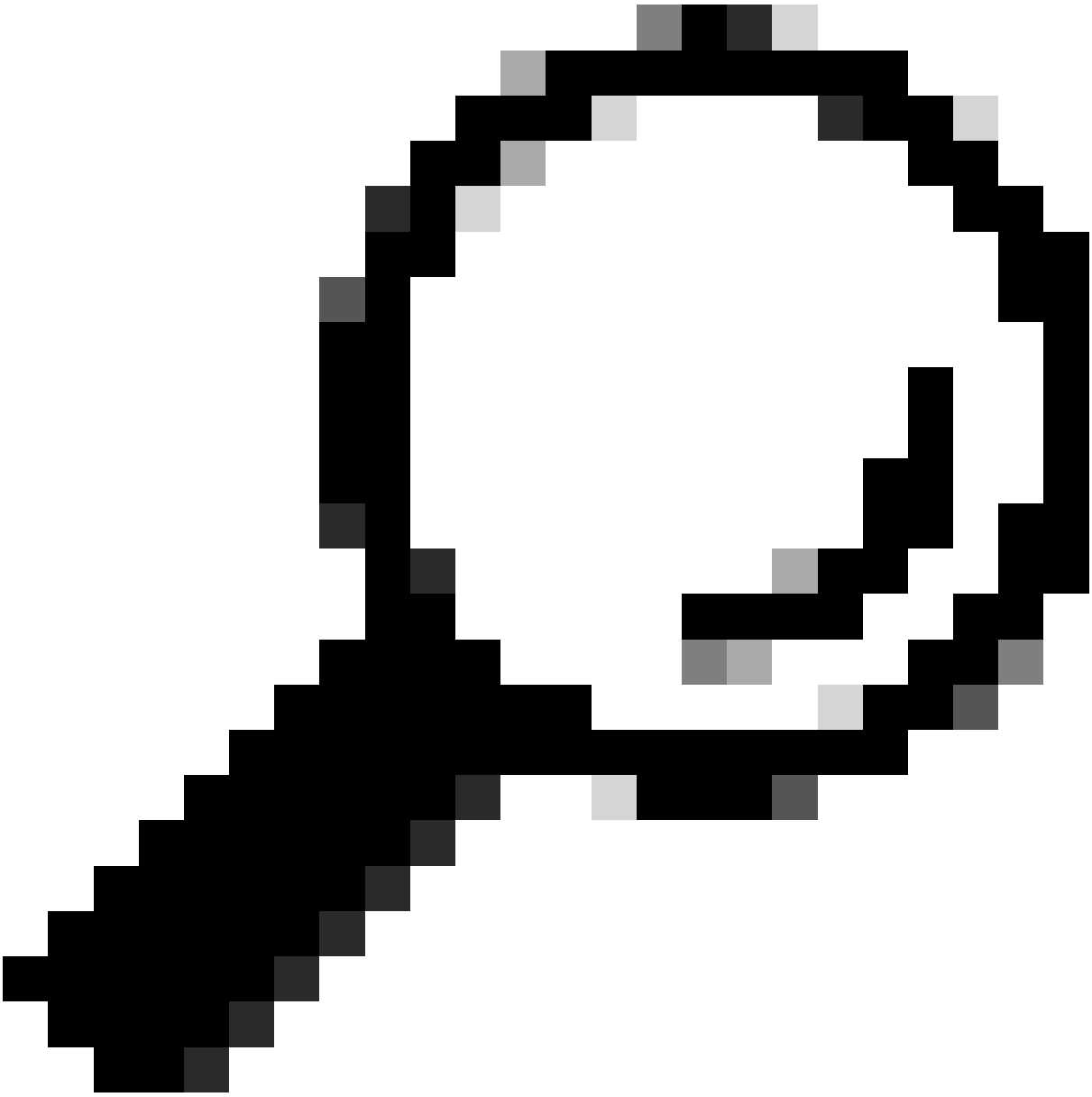
動態ARP檢測(DAI)

動態ARP檢測是一種安全功能，用於驗證網路中的ARP資料包。它會攔截、記錄並丟棄具有無效IP到MAC地址繫結的ARP資料包。此功能可保護網路免受某些中間人攻擊。

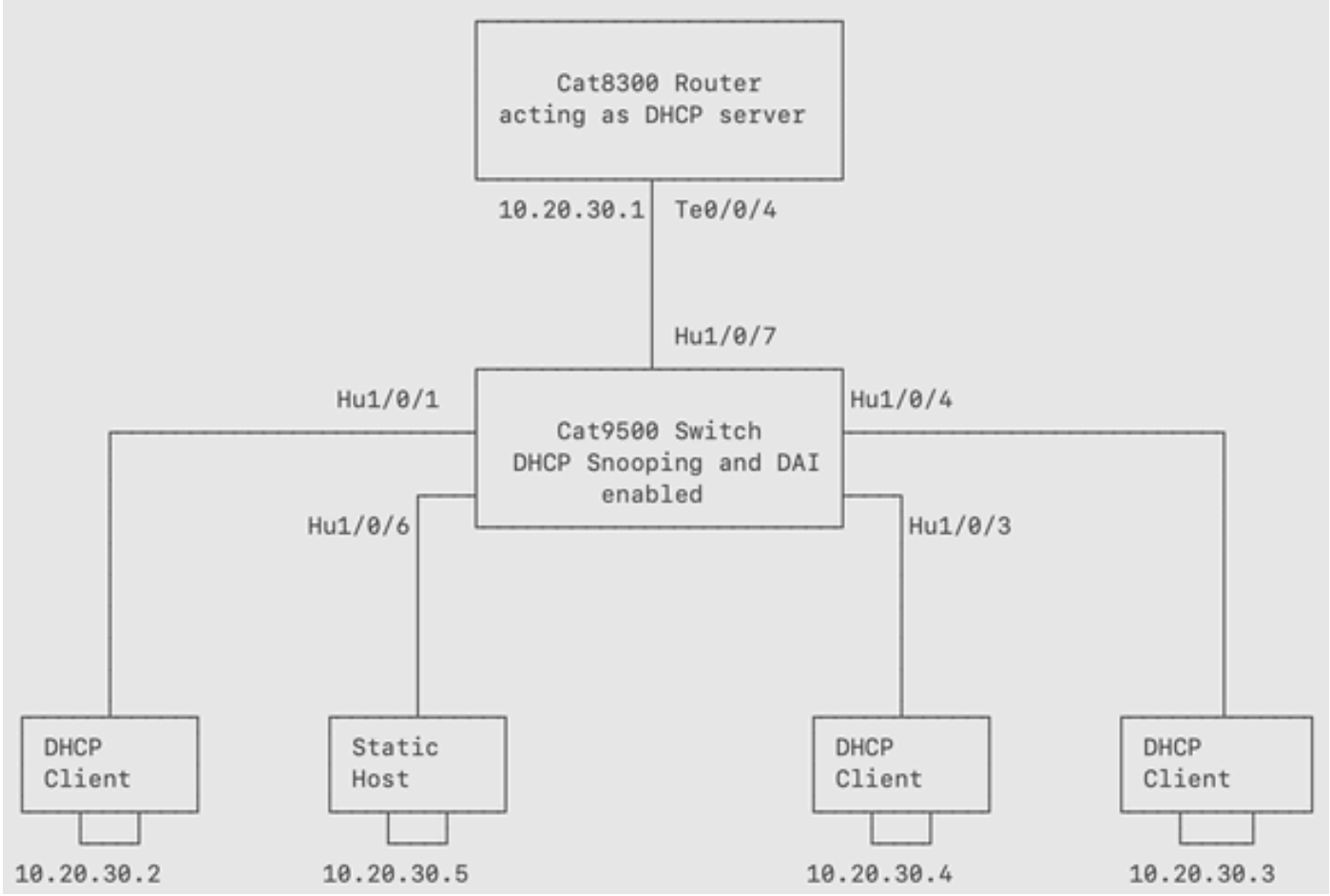
動態ARP檢測可確保只中繼有效的ARP請求和響應。交換機執行以下活動：

- 攔截不受信任埠上的所有ARP請求和響應
- 在更新本地ARP快取或將資料包轉發到相應目的地之前，驗證每個截獲的資料包是否都具有有效的IP到MAC地址繫結
- 丟棄無效的ARP資料包

動態ARP檢測根據儲存在受信任資料庫（即DHCP監聽繫結資料庫）中的有效IP到MAC地址繫結確定ARP資料包的有效性。
如果在VLAN和交換機上啟用了DHCP監聽，則此資料庫由DHCP監聽構建。如果在受信任的介面上收到ARP資料包，交換機將轉發該資料包而不進行任何檢查。
在不受信任的介面上，交換機僅當資料包有效時才轉發該資料包。



提示：**請參閱**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



此影像顯示連線到四台主機的Cat9500交換器，其中三台主機是DHCP使用者端，一台主機有靜態IP位址(10.20.30.5)。DHCP伺服器是配置了DHCP池的Cat8300系列路由器。

上述拓撲用於演示DAI如何檢測介面上的無效ARP請求並保護網路免遭惡意攻擊。

組態:

步驟 1.在交換機中全局配置DHCP監聽和DAI。

```
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
```

步驟 2.將連線到DHCP伺服器的介面Hu1/0/7配置為受信任埠。這將允許DHCP提供進入介面並隨後到達DHCP客戶端。

```
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
```

步驟 3.將連線到DHCP客戶端的埠配置為允許VLAN 10的接入埠。

```
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

步驟 4.驗證DHCP客戶端是否已從Cat9500交換機中的DHCP監聽繫結表接收到DHCP伺服器的IP地址。

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

您還可以檢查DHCP伺服器中的繫結。

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

第5步：將連線到Hu1/0/6的主機的IP地址從10.20.30.5更改為10.20.30.2，然後嘗試從該主機ping其他DHCP客戶端。

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

在Cat9500交換機上可以看到以下無效ARP日誌：

```
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
```

- 您可以看到，嘗試從Static_Host ping 10.20.30.3和10.20.30.4時，無法執行此操作。
儘管Static_Host試圖欺騙合法DHCP客戶端的IP地址，但它還是無法這樣做，因為到達Hu1/0/6的任何ARP資料包都將由交換機進行檢查，並與DHCP監聽繫結表中的資料進行比較。

- 來自Cat9500交換機的後續日誌確認從Static_Host傳送到DHCP客戶端的ARP請求被丟棄。

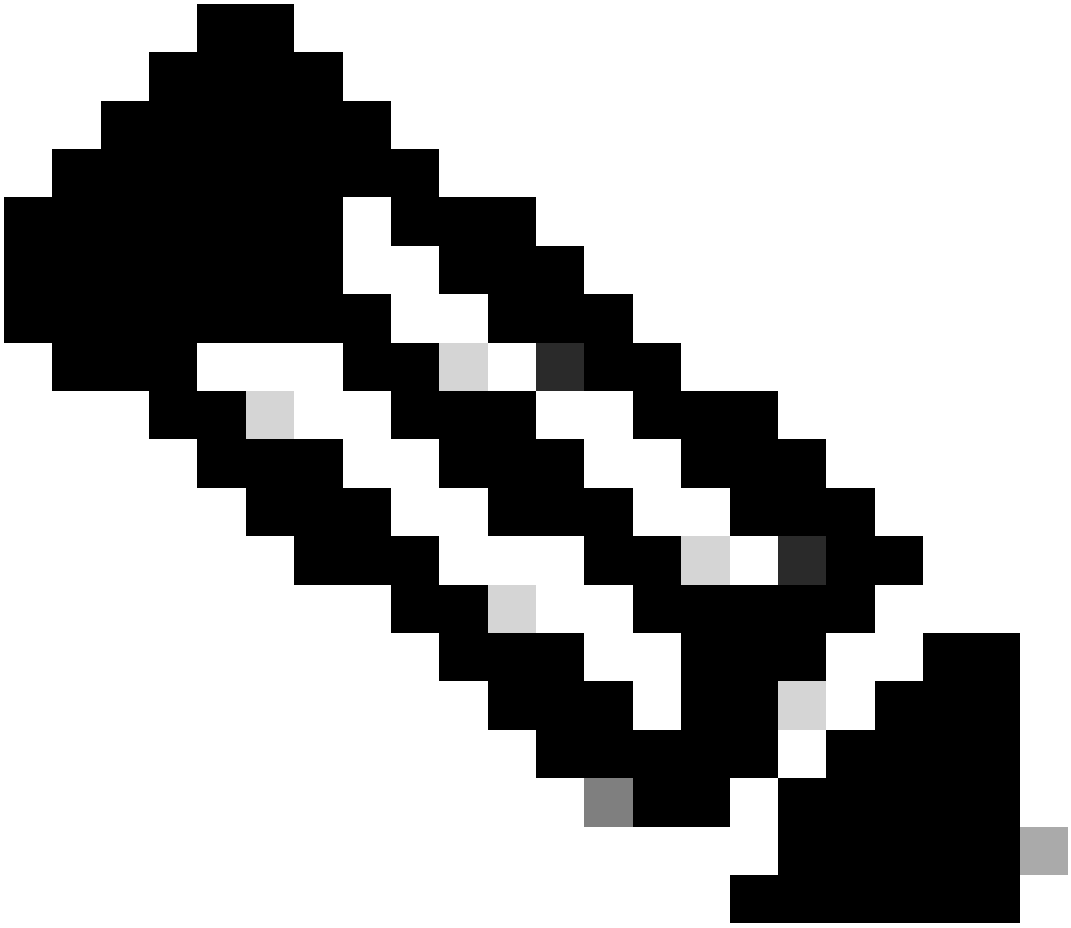
- Cat9500交換機透過參考DHCP監聽繫結資料庫來實現這一點。

- 當ARP請求進入源MAC-IP與DHCP監聽繫結資料庫中的值不匹配的Hu1/0/6時，交換機將丟棄該ARP請求。

步驟 6.驗證：

```
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
```

在此輸出中，您可以看到DAI在Cat9500交換機的VLAN 10中丟棄和允許的資料包數量。



註：一個非常重要的場景可能是網路中的合法主機為其分配了靜態IP地址（例如10.20.30.5）？

雖然主機沒有嘗試欺騙任何內容，但它仍然會與網路隔離，因為其MAC-IP繫結資料不在DHCP監聽繫結資料庫中。

這是因為靜態主機從未使用DHCP接收IP地址，因為它是靜態分配的。

我們可以實施一些解決方法，為具有靜態IP地址的合法主機提供連線。

選項 1.

使用ip arp inspection trust配置連線到主機的介面。

```
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
```

選項 2.

使用ARP Access-List允許靜態主機：

```
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

選項 3.

配置靜態主機的繫結表條目。

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提供的其他選項：

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

對於src-mac，請根據ARP正文中的傳送方MAC地址檢查乙太網報頭中的源MAC地址。此檢查會對ARP請求和響應執行。啟用時，具有不同MAC位址的封包會分類為無效且遭捨棄

對於dst-mac，請根據ARP主體中的目標MAC地址檢查乙太網報頭中的目標MAC地址。對ARP響應執行此檢查。啟用時，具有不同MAC位址的封包會分類為無效且遭捨棄。

對於IP，請檢查ARP主體中是否存在無效和未預期的IP地址。地址包括0.0.0.0、255.255.255.255和所有IP組播地址。在所有ARP請求和響應中檢查傳送方IP地址，僅在ARP響應中檢查目標IP地址。

您還可以配置ARP速率限制。預設情況下，不可信介面上的ARP流量限制為15 pps：

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

IP來源防護

- IPSG是一種安全功能，它透過根據DHCP監聽繫結資料庫和手動配置的IP源繫結過濾流量來限制非路由的第2層介面上的IP流量。
- 如果主機嘗試使用其鄰居的IP地址，您可以使用IPSG來防止流量攻擊。
- 在不受信任的介面上啟用DHCP監聽時，可以啟用IPSG。在介面上啟用IPSG後，交換機將阻止介面上接收的所有IP流量

，但DHCP監聽允許的DHCP資料包除外。

- 交換機在硬體中使用源IP查詢表將IP地址繫結到埠。對於IP和MAC過濾，使用源IP和源MAC查詢的組合。允許繫結表中具有源IP地址的IP流量，但拒絕所有其他流量。

- IP源繫結表包含由DHCP監聽獲得的繫結或手動配置的繫結（靜態IP源繫結）。此表格中的專案包含IP位址、其關聯的MAC位址與其關聯的VLAN編號。只有啟用IP源防護時，交換機才會使用IP源繫結表。

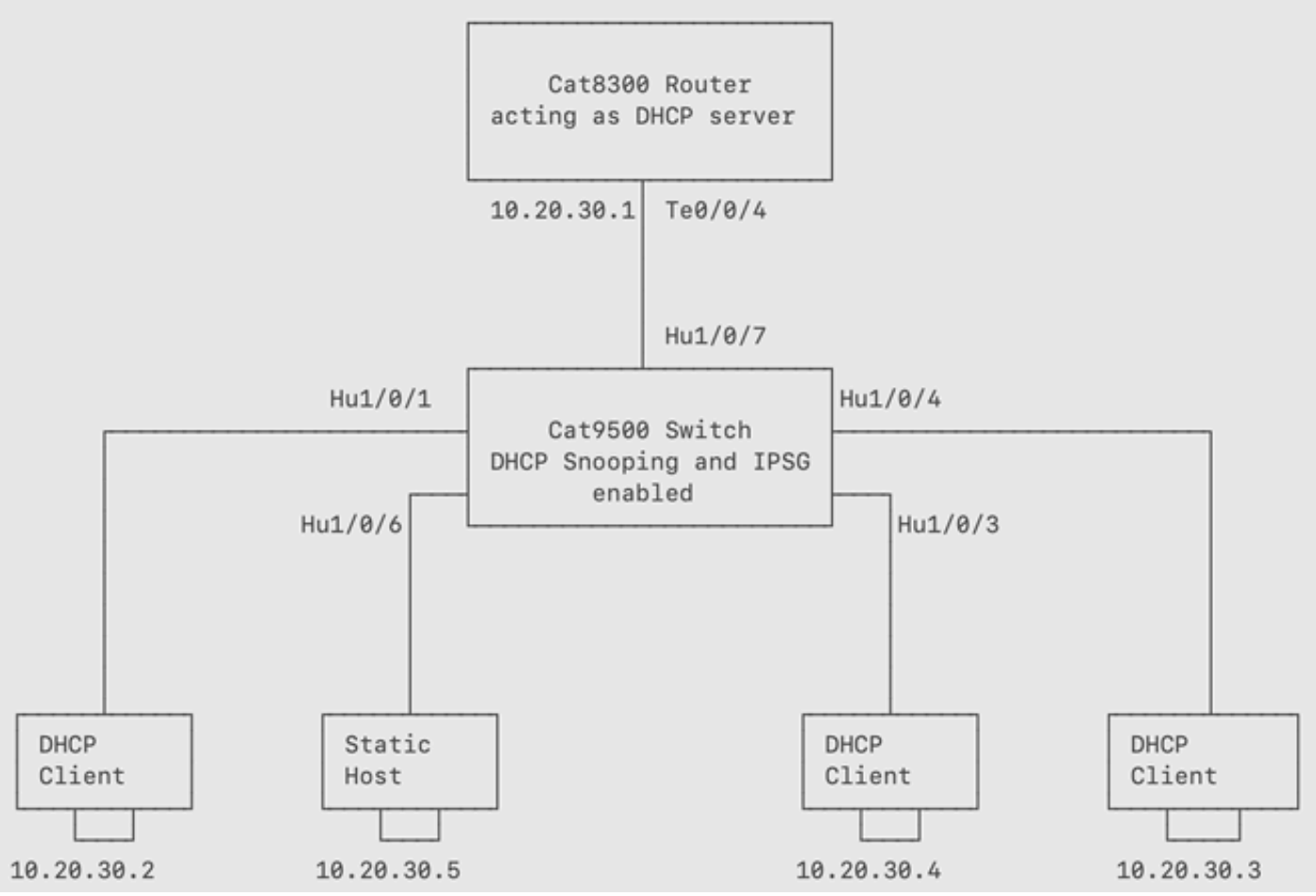
- 您可以使用源IP地址過濾或源IP和MAC地址過濾來配置IPSG。

適用於靜態主機的IPSG

- 靜態主機的IPSG允許IPSG在沒有DHCP的情況下工作。靜態主機的IPSG依賴IP裝置跟蹤表條目來安裝埠ACL。交換機根據ARP請求或其他IP資料包建立靜態條目，以維護給定埠的有效主機清單。

參考資料：

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交換機連線到4台主機，其中3台主機是DHCP客戶端，1台主機具有靜態IP地址。DHCP伺服器是配置了DHCP池的Cat8300系列路由器。

您可以使用此拓撲來演示IPSG如何檢測並阻止來自MAC-IP繫結未出現在DHCP監聽繫結資料庫中的主機的流量。

設定:

步驟 1.在Cat9500交換機中全局配置DHCP監聽。

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

步驟 2.將連線到DHCP伺服器的介面Te1/0/7配置為受信任埠。這允許DHCP提供進入介面並隨後到達DHCP客戶端。

```
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
```

步驟 3.將連線到DHCP客戶端的埠配置為允許VLAN 10的接入埠。

```
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
```

步驟 4.驗證DHCP客戶端是否已從DHCP伺服器收到IP地址。

```
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

步驟 5.在連線到所有終端主機（3個DHCP客戶端和1個具有靜態IP地址的主機）的介面下配置IPSG。

```
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

驗證：

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

從該輸出中，您可以看到Hu1/0/6的IP Address欄位設定為deny-all，因為DHCP監聽繫結表中沒有與此介面對應的MAC-IP繫結。

步驟 6.嘗試從 Static_Host ping IP**地址為**10.20.30.2、10.20.30.3**和**10.20.30.4**的**DHCP**客戶端。

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提供的其他選項：

預設情況下，IPSG僅根據IP地址過濾不受信任埠上的傳入流量。
如果要根據IP和MAC地址執行過濾，請執行以下步驟。

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

在此輸出中，您可以看到Filter-type為ip-mac。因此，交換機現在可根據源IP和MAC地址過濾這些介面上的傳入資料包。

DAI和IPSG的故障排除提示

- 在排除DAI和IPSG相關問題故障時，首先要檢查的是驗證DHCP監聽繫結表是否已正確填充。
- 在啟用這些功能之前，請使用靜態IP地址處理終端。如果不想讓這些裝置失去可達性，請配置靜態繫結，或採用上述方法之一使交換機信任這些終端。
- 在尚未啟用DHCP監聽且客戶端已經從DHCP伺服器接收IP的環境中配置DAI或IPSG時，首先啟用DHCP監聽並執行以下兩個步驟之一：
  - 退回客戶端連線的介面，以便其續訂租期。
  - 等待客戶端自動續訂租期。這可能需要花費更多時間，但省去了手動退回所有客戶端連線的埠的麻煩。
- 執行上述兩個步驟中的任何一個都將觸發新的DORA事務。交換機將嗅探DORA資料包並更新繫結表。如果未執行此操作，並且在配置DHCP監聽後立即啟用DAI或IPSG，則可能會遇到網路中所有DHCP客戶端都失去與網路的連線的問題。
- 在配置DAI或IPSG的環境中排除連線問題故障時，請確保DHCP監聽繫結表未損壞。確保交換機可以訪問儲存此表的資料結構。
- 某些情況下，繫結表可能會導出到交換機啟動後需要一段時間才能初始化的介質，或者由於某種原因導致交換機無法訪問該介質。在這些情況下，您可能已經觀察到連線問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。