Catalyst交换机中的动态ARP检测(DAI)和IP源保护(IPSG)故障排除

目录

简介

本文档介绍动态ARP检测(DAI)和IP源保护(IPSG)的工作原理，以及如何在Catalyst 9K交换机中验证它们。

DHCP监听及相关功能

在深入了解DAI和IPSG之前，您需要简要讨论DHCP监听，这是DAI和IPSG的前提条件。

动态主机配置协议(DHCP)是一种客户端/服务器协议，可自动为互联网协议(IP)主机提供其IP地址和其它相关配置信息（如子网掩码和默认网关）。RFC 2131和2132将DHCP定义为基于Bootstrap协议(BOOTP)的Internet工程任务组(IETF)标准，BOOTP是DHCP共享许多实施细节的协议。DHCP允许主机从DHCP服务器获取所需的TCP/IP配置信息。

DHCP监听是一种安全功能，作用类似于不可信主机和可信DHCP服务器之间的防火墙。DHCP监听功能执行以下活动：

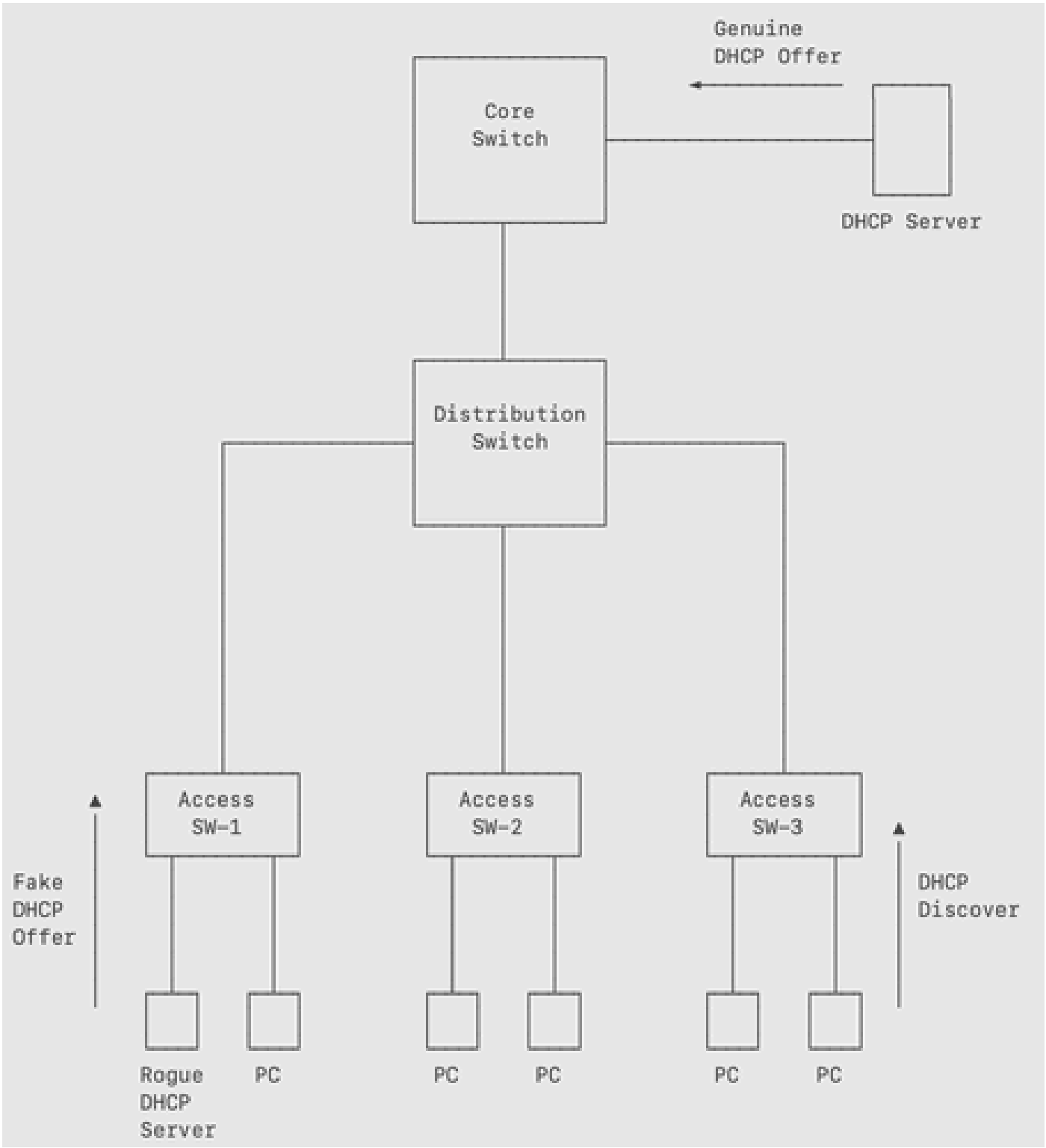
- 验证从不可信源接收的DHCP消息并过滤出无效消息。
- 对来自受信任和不受信任源的DHCP流量进行速率限制。
- 建立并维护DHCP监听绑定数据库，其中包含有关使用租用IP地址的不受信任主机的信息。
- 使用DHCP监听绑定数据库验证来自不受信任主机的后续请求。

DAI是一种安全功能，用于验证网络中的地址解析协议(ARP)数据包。DAI允许网络管理员拦截、记录和丢弃MAC地址与IP地址绑定无效的ARP数据包。此功能可保护网络免受某些“中间人”攻击。

IPSG是一项安全功能，它通过根据DHCP监听绑定数据库和手动配置的IP源绑定过滤流量来限制非路由的第2层接口上的IP流量。如果主机尝试使用其邻居的IP地址，您可以使用IPSG来防止流量攻

击。

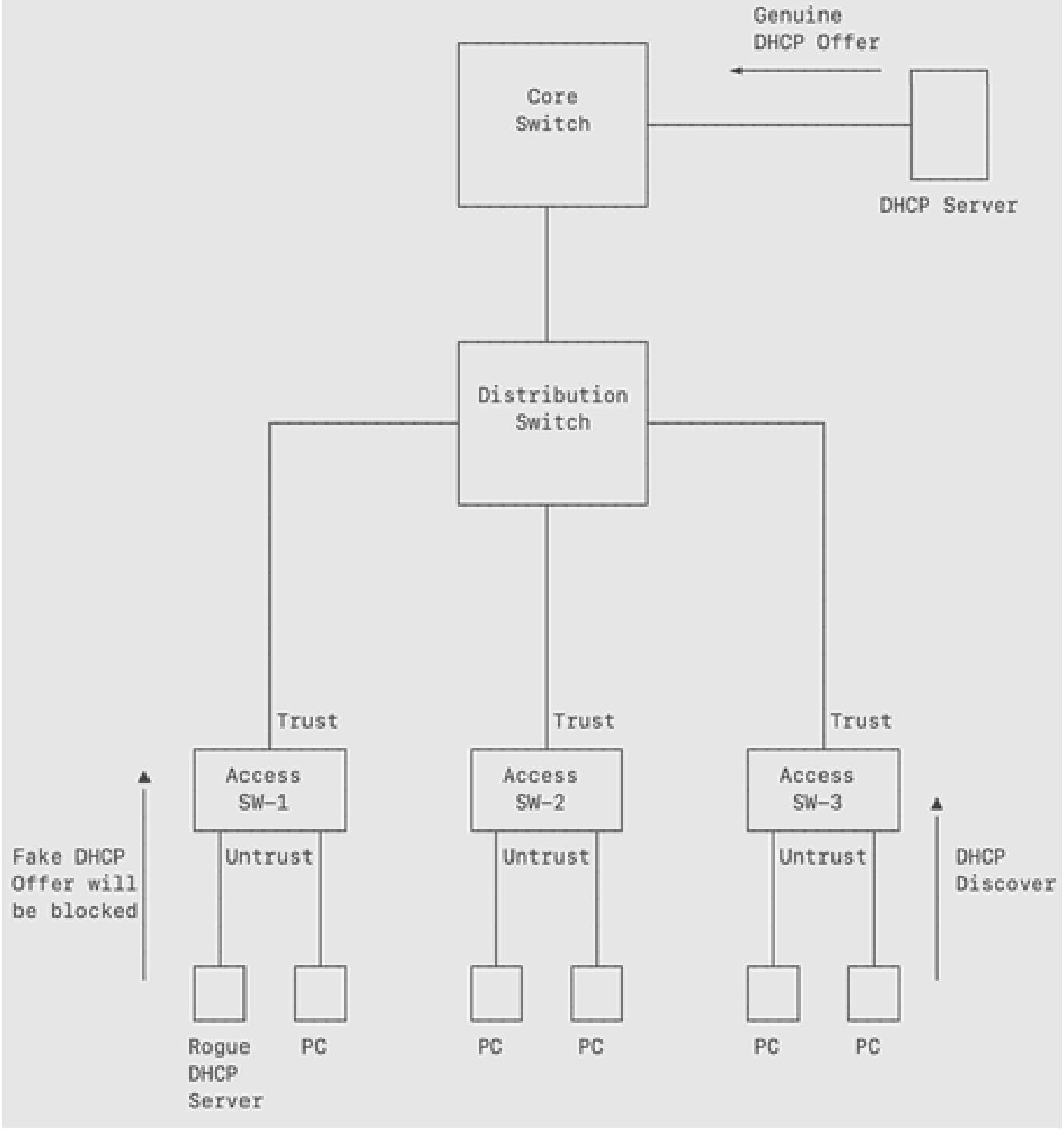
没有DHCP监听的场景



1. 在此图中，您可以看到多个客户端希望从连接到核心交换机的DHCP服务器接收IP地址。
2. 但是，有一个恶意/恶意DHCP服务器连接到一台接入层交换机，该交换机可以接收DHCP发现并发送DHCP提供，其速度比实际DHCP服务器更快。

3. 攻击者可以设置要约消息中的网关地址，使其接收来自客户端的所有流量，从而损害通信的机密性。
4. 这被称为“中间人”攻击。

使用DHCP监听的方案

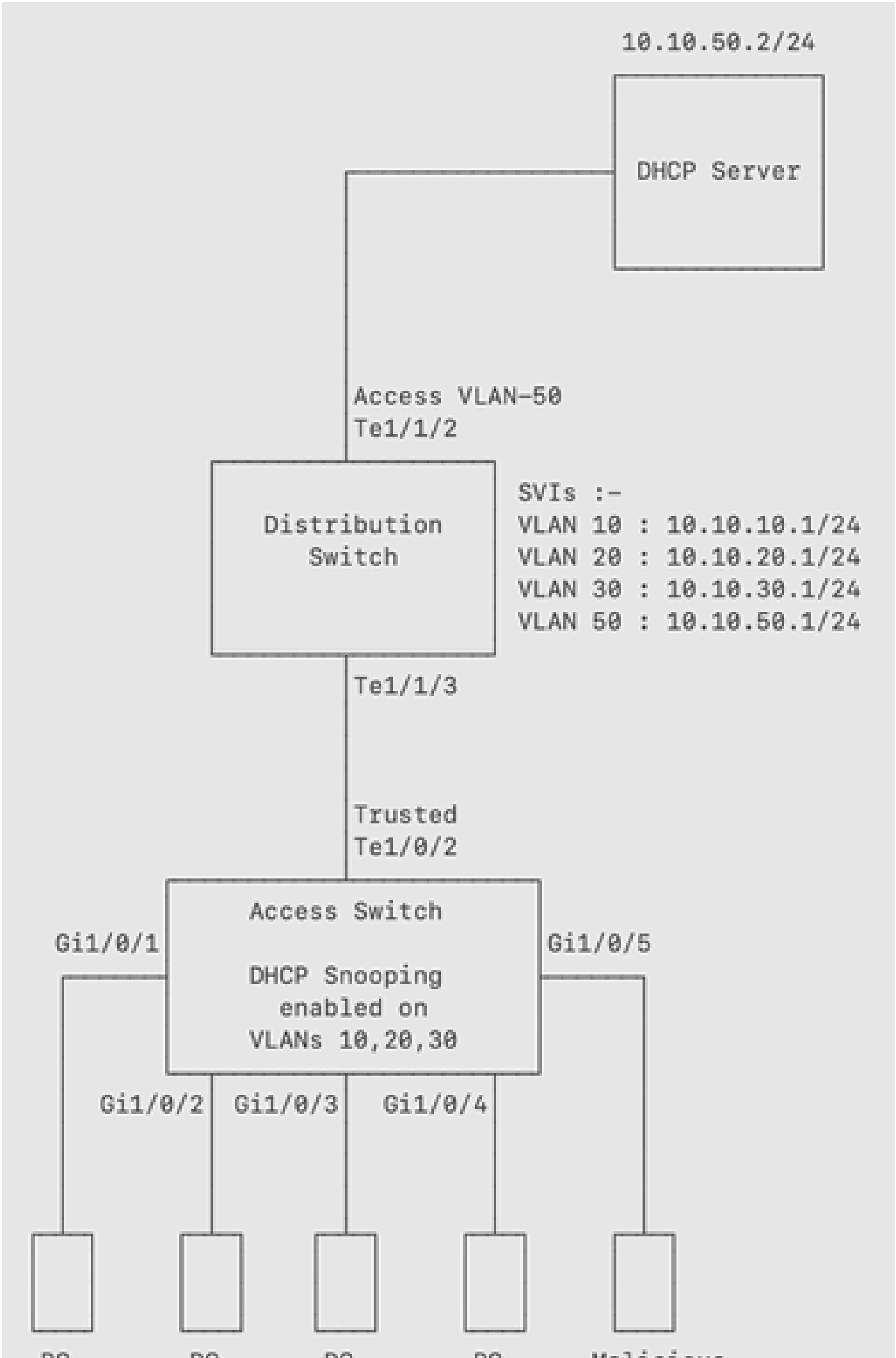


1. 通过在接入交换机中启用DHCP侦听，将交换机配置为侦听DHCP流量并阻止在不可信端口上收到的任何恶意DHCP数据包。
2. 一旦在交换机中启用DHCP监听，所有接口都会自动变为不可信状态。
3. 将连接到终端设备的端口设置为不可信，并将连接到正版DHCP服务器的端口配置为可信。

4. 不受信任的接口将阻止DHCP提供消息。DHCP提供消息仅在受信任端口上被允许。
5. 您可以限制终端主机每秒可以发送到不受信任接口的DHCP发现数据包的数量。 这是一种安全机制，可保护DHCP服务器，防止出现大量传入DHCP发现，从而立即耗尽地址池。

本节介绍如何在交换网络中配置DHCP监听：

拓扑：


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
```

第二步：在接收来自正版DHCP服务器的DHCP提供的访问交换机的所有接口上配置DHCP监听信任。此类接口的数量取决于网络设计和DHCP服务器的放置。这些接口将指向正版DHCP服务器。

接入层交换机:

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

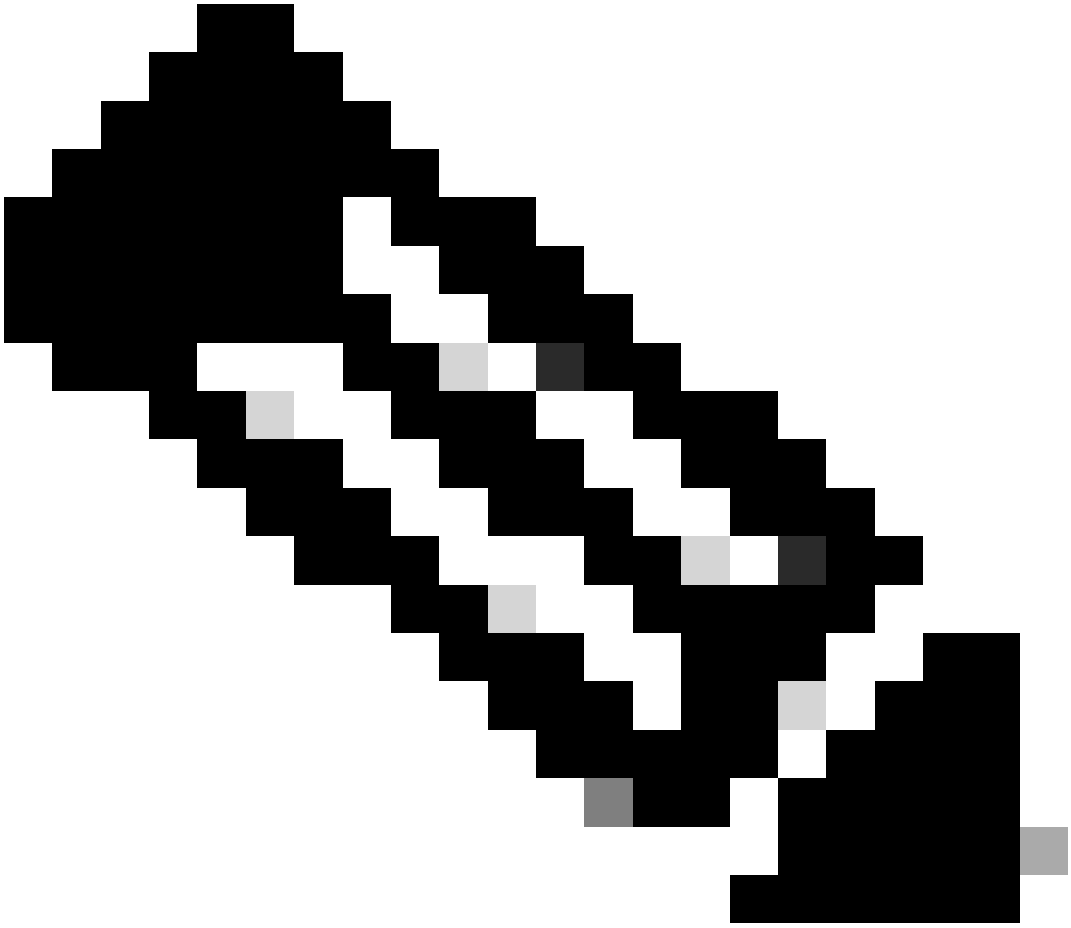
第三步：一旦全局配置DHCP监听，交换机中的所有端口都会自动变为不可信状态（手动信任的端口除外，如前所示）。但是，可以配置终端主机每秒可以发送到不受信任接口的DHCP发现数据包的数量。
这是一种安全机制，可保护DHCP服务器，防止出现大量传入DHCP发现，从而立即耗尽地址池。

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

验证：

```
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：查看此输出时，您会看到在**show ip dhcp snooping** 输出中，连接到恶意DHCP服务器的Gi1/0/5被称为不受信任。

因此，DHCP监听将对这些端口执行所有检查。
例如，这将导致该端口(Gi1/0/5)上的所有传入DHCP提供被丢弃。

以下是DHCP监听绑定表，显示Gi1/0/1、Gi1/0/2、Gi1/0/3上3个客户端的IP地址、MAC地址和接口：

```
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
```

出于演示目的，ip dhcp snooping trust将配置从接入交换机的Te1/0/2下移除。请查看在Switch：中生成的日志

```
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
```

- 您可以看到，接入交换机在Te1/0/2上丢弃传入的DHCP提供数据包，因为它不再受信任。
- 日志中的MAC地址属于VLAN 10、20和30的SVI，因为它们是从DHCP服务器向这些客户端发送这些提供的地址的客户端。

ARP 毒化

ARP通过将IP地址映射到MAC地址来提供第2层广播域内的IP通信。该协议很简单，但容易遭受称为ARP毒化的攻击。

ARP毒化攻击是指攻击者在网络上发送虚假的ARP应答数据包。

恶意用户可以通过毒化连接到子网的系统的ARP缓存并拦截流向子网上其他主机的流量来攻击连接到第2层网络的主机、交换机和路由器

这是典型的中间人攻击。

预防机制

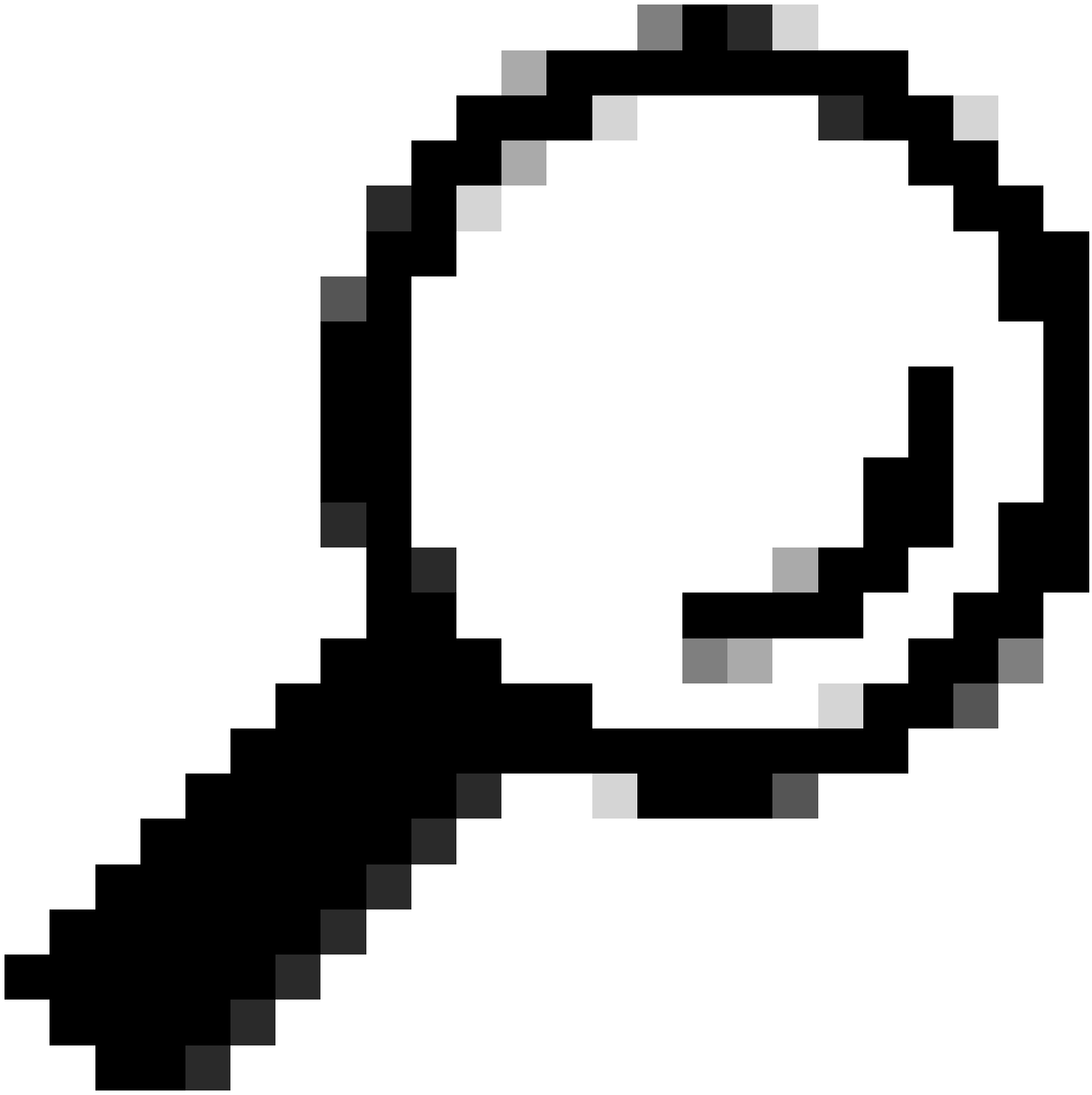
动态ARP检测(DAI)

动态 ARP 检测是一项安全功能，用于验证网络中的 ARP 数据包。它拦截、记录并丢弃具有 IP 到 MAC 地址的无效绑定的 ARP 数据包。使用此功能可以防止网络受到某些中间人攻击。

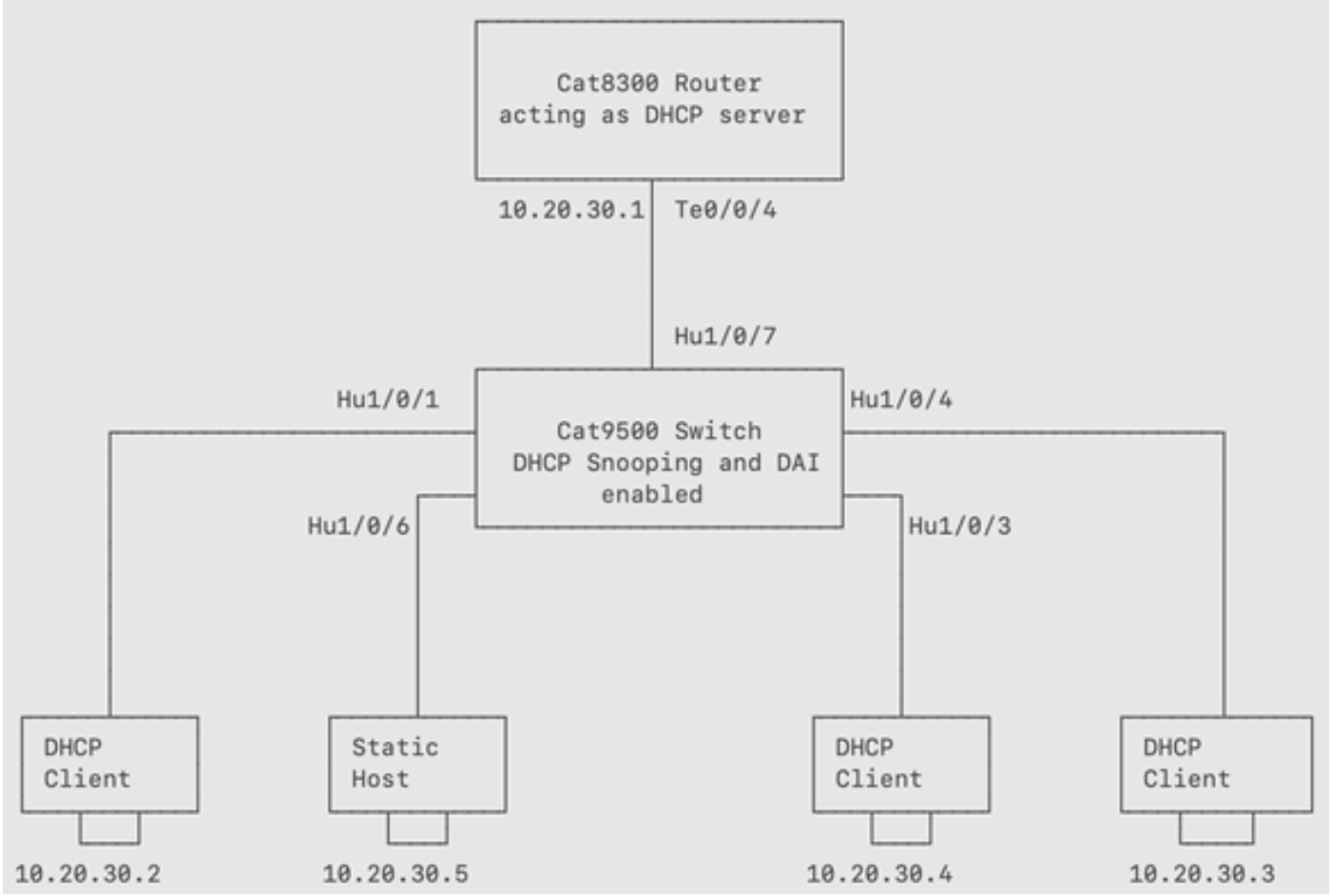
动态 ARP 检测可确保仅转发有效 ARP 请求和响应。交换机可执行以下活动：

- 拦截不受信任端口上的所有 ARP 请求和响应
- 在更新本地ARP缓存或将数据包转发到相应目的地之前，验证这些截获的数据包中是否每个数据包都具有有效的IP到MAC地址绑定
- 丢弃无效的 ARP 数据包

动态 ARP 检测可根据受信任数据库（DHCP 监听绑定数据库）中存储的 IP 到 MAC 地址的有效绑定来确定 ARP 数据包的有效性。如果已在 VLAN 和交换机上启用 DHCP 监听，则此数据库可通过 DHCP 监听来构建。如果在受信任接口上收到 ARP 数据包，交换机将在不做任何检查的情况下转发数据包。
在不受信任接口上，交换机仅转发有效数据包。



提示：请参阅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



此映像演示连接到四台主机的Cat9500交换机，其中3台主机是DHCP客户端，1台主机具有静态IP地址(10.20.30.5)。DHCP服务器是配置有DHCP池的Cat8300系列路由器。

上述拓扑用于演示DAI如何检测接口上的无效ARP请求并保护网络免受恶意攻击者的攻击。

配置:

步骤1:在交换机中全局配置DHCP监听和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
```

第二步：将连接到DHCP服务器的接口Hu1/0/7配置为可信端口。这将允许DHCP提供进入接口并随后到达DHCP客户端。

```
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
```

第三步：将连接到DHCP客户端的端口配置为允许VLAN 10的接入端口。

```
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

第四步：验证DHCP客户端是否已从Cat9500交换机的DHCP监听绑定表中收到来自DHCP服务器的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

您还可以检查DHCP服务器中的绑定。

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：将连接到Hu1/0/6的主机的IP地址从10.20.30.5更改为10.20.30.2，然后尝试从该主机ping其他DHCP客户端。

```
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交换机上可以看到以下无效ARP日志：

```
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
```

- 如您所见，当您尝试从Static_Host ping 10.20.30.3和10.20.30.4时，您做不到。
即使Static_Host试图欺骗合法DHCP客户端的IP地址，它也无法这样做，因为到达Hu1/0/6的任何ARP数据包将由交换机进行检查，并与DHCP监听绑定表中的数据进行比较。

- 来自Cat9500交换机的后续日志确认从Static_Host发送到DHCP客户端的ARP请求被丢弃。

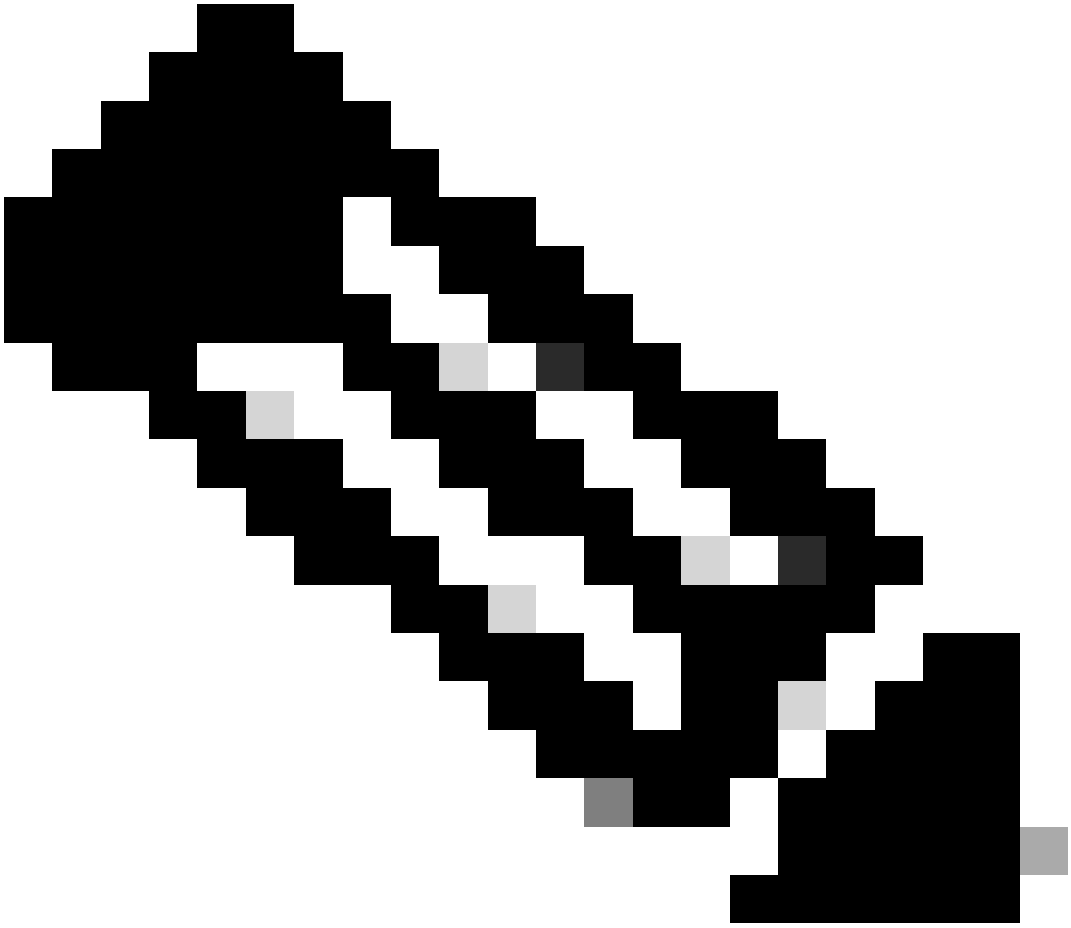
- Cat9500交换机通过引用DHCP监听绑定数据库来实现这一点。

- 当ARP请求进入Hu1/0/6且源MAC-IP与DHCP监听绑定数据库中的值不匹配时，交换机将丢弃该ARP请求。

第六步：验证：

```
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
```

在此输出中，您可以看到Cat9500交换机中VLAN 10中的DAI丢弃和允许的数据包数量。



注意：一个非常重要的场景可能是网络中的合法主机为其分配了静态IP地址（例如10.20.30.5）？

尽管主机没有尝试伪装任何内容，但仍会与网络隔离，因为其MAC-IP绑定数据不存在于DHCP监听绑定数据库中。

这是因为静态主机从未使用DHCP接收IP地址，因为它是静态分配的。

我们提供了几种解决方法，可以通过这些解决方法为具有静态IP地址的合法主机提供连接。

第 1 项.

使用ip arp inspection trust配置连接到主机的接口。

```
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
```

第 2 项.

通过使用ARP Access-List允许静态主机：

```
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

选项 3.

配置静态主机的绑定表条目。

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提供的其他选项：

```
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
```

对于src-mac，请根据ARP正文中的发送方MAC地址检查以太网报头中的源MAC地址。对ARP请求和响应执行此检查。启用时，具有不同MAC地址的数据包将被分类为无效并丢弃

对于dst-mac，请根据ARP正文中的目标MAC地址检查以太网报头中的目标MAC地址。对ARP响应执行此检查。启用后，具有不同MAC地址的数据包将被分类为无效并丢弃。

对于IP，检查ARP正文是否存在无效和意外的IP地址。地址包括0.0.0.0、255.255.255.255和所有IP组播地址。在所有ARP请求和响应中检查发送方IP地址，仅在ARP响应中检查目标IP地址。

您还可以配置ARP速率限制。默认情况下，不可信接口上的ARP流量限制为15 pps：

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

IP 源防护

- IPSG是一项安全功能，它通过根据DHCP监听绑定数据库和手动配置的IP源绑定过滤流量来限制非路由第2层接口上的IP流量。
- 如果主机尝试使用其邻居的IP地址，您可以使用IPSG来防止流量攻击。
- 在不受信任的接口上启用DHCP监听时，可以启用IPSG。在接口上启用IPSG后，交换机将阻止接口上接收的所有IP流量

，但DHCP监听允许的DHCP数据包除外。

- 交换机使用硬件中的源IP查找表将IP地址绑定到端口。对于IP和MAC过滤，使用源IP和源MAC查找的组合。允许绑定表中具有源IP地址的IP流量，而拒绝所有其他流量。

- IP 源绑定表中包含由 DHCP 监听识别的绑定或手动配置的绑定（静态 IP 源绑定）。此表中的条目具有 IP 地址、关联的 MAC 地址和关联的 VLAN 编号。只有启用IP源防护时，交换机才会使用IP源绑定表。

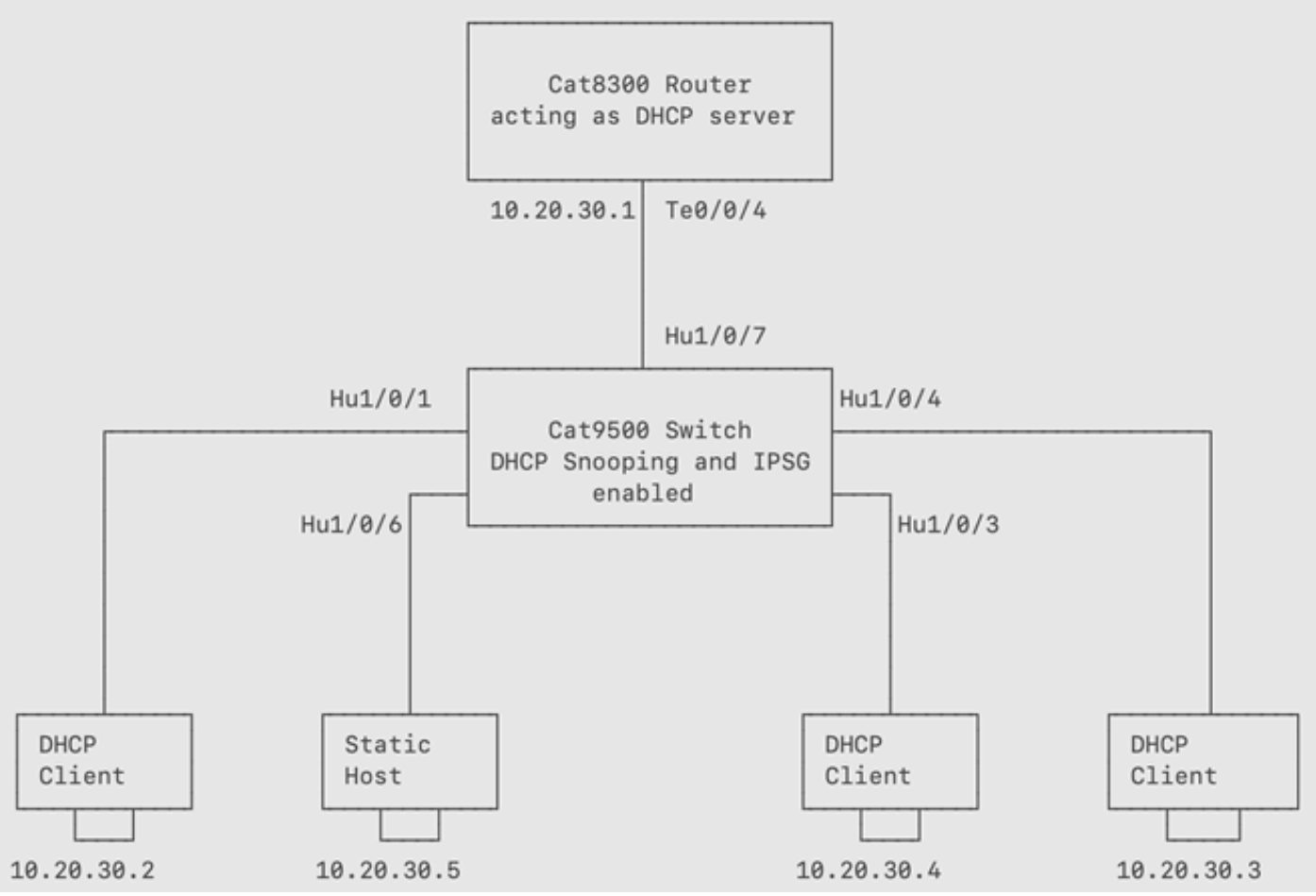
- 您可以使用源IP地址过滤或源IP和MAC地址过滤来配置IPSG。

静态主机的IPSG

- 静态主机的IPSG允许IPSG在没有DHCP的情况下工作。静态主机的IPSG依赖IP设备跟踪表条目安装端口ACL。交换机根据ARP请求或其他IP数据包创建静态条目，以维护给定端口的有效主机列表。

参考:

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交换机连接到4台主机，其中3台主机是DHCP客户端，1台主机具有静态IP地址。DHCP服务器是配置有DHCP池的Cat8300系列路由器。

可以使用此拓扑演示IPSG如何检测和阻止MAC-IP绑定未出现在DHCP监听绑定数据库中的主机的流量。

配置:

步骤1:在Cat9500交换机中全局配置DHCP监听。

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

第二步：将连接到DHCP服务器的接口Te1/0/7配置为可信端口。这允许DHCP提供进入接口并随后到达DHCP客户端。

```
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
```

第三步：将连接到DHCP客户端的端口配置为允许VLAN 10的接入端口。

```
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
```

第四步：验证DHCP客户端是否已从DHCP服务器收到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

第五步：在连接到所有终端主机（3个DHCP客户端和1个使用静态IP地址的主机）的接口下配置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

验证：

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

从该输出中，您可以看到Hu1/0/6的IP Address字段设置为deny-all，因为DHCP监听绑定表中没有与此接口对应的MAC-IP绑定。

第六步：尝试从Static_Host ping IP地址为10.20.30.2、10.20.30.3和10.20.30.4的DHCP客户端。

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提供的其他选项：

默认情况下，IPSG仅根据IP地址过滤不可信端口上的传入流量。
如果要根据IP和MAC地址执行过滤，请执行以下步骤。

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

在此输出中，您可以看到Filter-type为ip-mac。因此，交换机现在会根据源IP地址和MAC地址过滤这些接口上的传入数据包。

DAI和IPSG的故障排除提示

- 在排查DAI和IPSG相关问题故障时，首先要检查的是验证是否已正确填充DHCP监听绑定表。
- 在启用这些功能之前，请使用静态IP地址处理终端。如果不想让这些设备失去可达性，请配置静态绑定或使用前面提到的方法之一使交换机信任这些终端。
- 在尚未启用DHCP监听的环境中配置DAI或IPSG时，客户端已经从DHCP服务器收到IP，请首先启用DHCP监听并执行下列两个步骤之一：
  - 退回客户端连接的接口，以便其续订租期。
  - 等待客户端自动续订租期。这可能需要更长的时间，但省去了手动退回所有客户端连接的端口的麻烦。
- 执行上述两个步骤中的任何一个都将触发新的DORA事务。交换机将嗅探DORA数据包并更新绑定表。如果未执行此操作，并且在配置DHCP监听后立即启用DAI或IPSG，则可能会遇到网络中所有DHCP客户端都失去与网络的连接的问题。
- 在配置了DAI或IPSG的环境中排除连接问题时，请确保DHCP监听绑定表未损坏。确保交换机可以访问存储此表的数据结构。
- 在某些情况下，绑定表可能会导出到交换机启动后需要一段时间才能初始化的介质，或者由于某种原因交换机无法访问该介质。您可能观察到了此类场景中的连接问题。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。