驗證交換機上的IP裝置跟蹤後MAB配置

目錄

簡介

本文檔介紹MAB配置後IP裝置跟蹤的行為以及MAB身份驗證後通訊問題的可能解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務引擎的配置
- Cisco Catalyst的配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分辨識服務引擎虛擬3.3修補程式1
- C1000-48FP-4G-L 15.2(7)E9

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

圖表

本文檔介紹此圖中MAB身份驗證的配置與驗證。
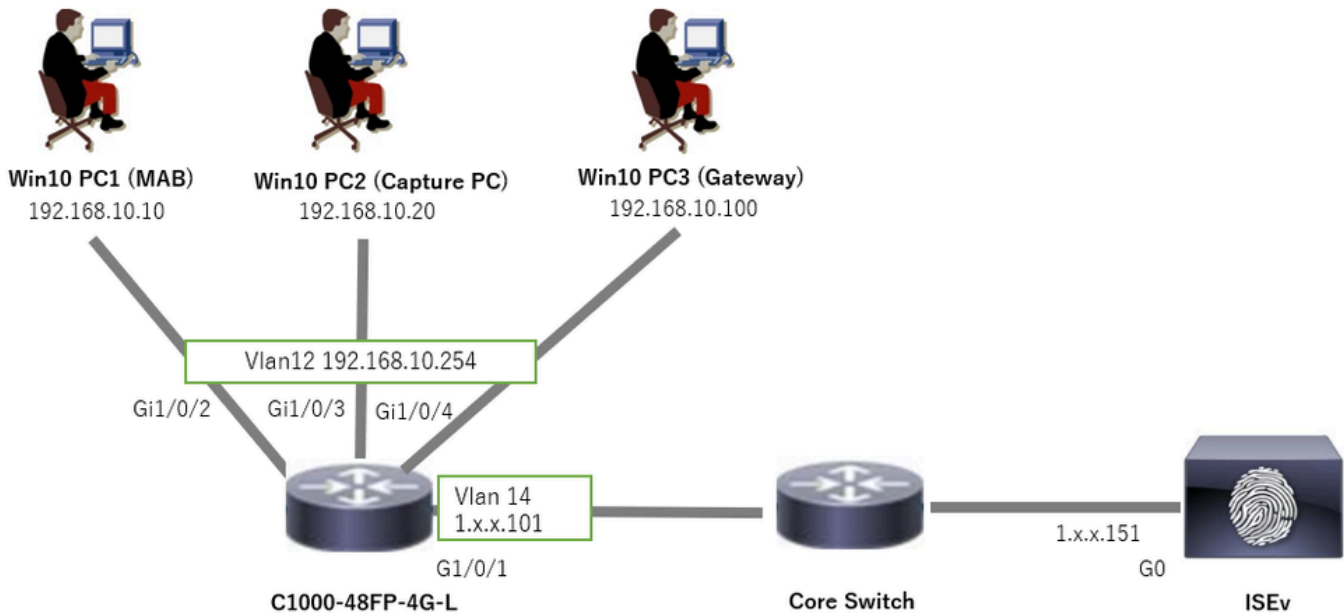
網路圖表

背景資訊

即使MAB身份驗證成功，但在重新引導（或拔掉並重新插入電纜）Win10 PC1後，它仍無法成功ping通網關(Win10 PC3)。此意外行為是由於Win10 PC1上的IP地址衝突引起的。
預設情況下，IP裝置跟蹤及其ARP探測功能在配置為MAB的介面上啟用。當Windows PC連線到已啟用IP裝置跟蹤的Catalyst交換機時，Windows端可能會檢測到IP地址衝突。 出現這種情況是因為在此機制的檢測窗口期間收到ARP探測（傳送方IP地址為0.0.0.0），將其視為IP地址衝突。

組態

此配置示例演示了MAB配置後IP裝置跟蹤的行為。

C1000中的配置

這是C1000 CLI中的最小配置。

```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123

aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan12
ip address 192.168.10.254 255.255.255.0

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
Switch port access vlan 12
Switch port mode access

interface GigabitEthernet1/0/4
Switch port access vlan 12
Switch port mode access

interface GigabitEthernet1/0/2
Switch port access vlan 12
Switch port mode access
authentication host-mode multi-auth
authentication port-control auto
spanning-tree portfast edge
mab

// for packet capture
monitor session 1 source interface Gi1/0/2
monitor session 1 destination interface Gi1/0/3
```

ISE中的配置

步驟 1.增加裝置

導航到管理>網路裝置，點選增加按鈕以增加C1000裝置。

- 名稱：C1000
- IP地址：1.x.x.101

增加裝置

步驟 2.增加終結點

導航到情景可視性>端點，點選增加按鈕以增加端點的MAC。
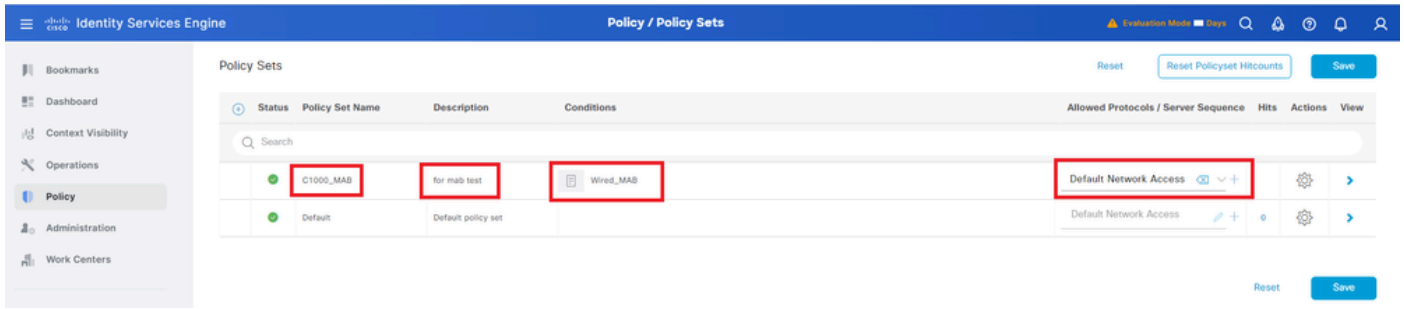

增加終結點

步驟 3.增加策略集

導航到策略>策略集，點選+ 增加策略集。

- 策略集名稱：C1000_MAB
- 描述：用於mab測試

- 條件：Wired_MAB
- 允許的協定/伺服器序列：預設網路訪問

增加策略集

步驟 4.增加身份驗證策略

導航到策略集，點選C1000_MAB增加身份驗證策略。

- 規則名稱：MAB_authentication
- 條件：Wired_MAB
- 使用：內部終端
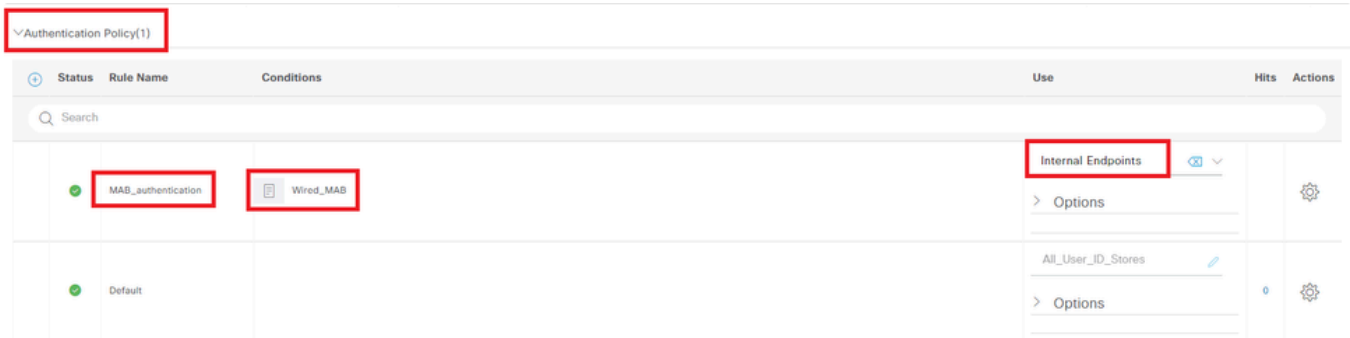
增加身份驗證策略

步驟 5.增加授權策略

導航到策略集，點選C1000_MAB增加授權策略。

- 規則名稱：MAB_authorization
- 條件： Network_Access_Authentication_Passed
- 結果：PermitAccess
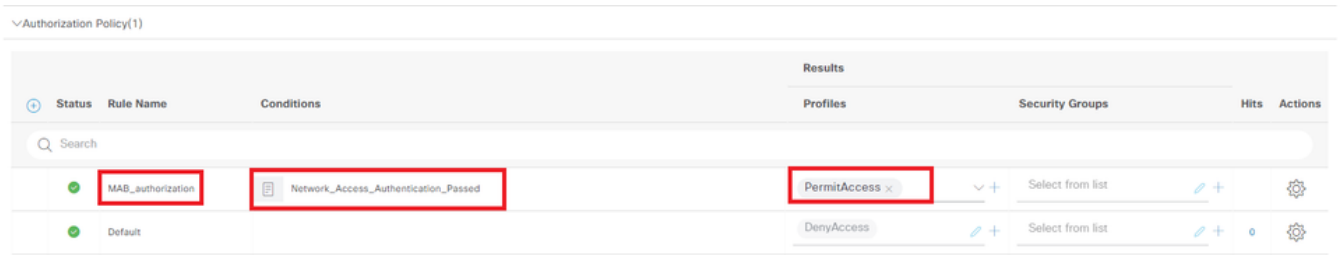
增加授權策略

驗證

配置MAB之前

運行show ip device tracking all命令以確認IP裝置跟蹤功能已停用。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Disabled

```
-------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-------------------------------------------------------------------------------------------
```

配置MAB之後

步驟 1.MAB驗證之前

運行show ip device tracking all命令以確認是否啟用了IP裝置跟蹤功能。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Enabled

```
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
-------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-------------------------------------------------------------------------------------------

Total number interfaces enabled: 1
Enabled interfaces:
  Gi1/0/2
```

步驟 2.MAB驗證之後

從Win10 PC1初始化MAB身份驗證並運行show ip device tracking all命令以確認GigabitEthernet1/0/2上IP裝置跟蹤的狀態。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Enabled

Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0

IP Address MAC Address Vlan Interface Probe-Timeout State Source
----

192.168.10.10

 b496.9115.84cb 12 GigabitEthernet1/0/2 30

ACTIVE

 ARP

Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2

步驟 3.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/2 details命令以確認MAB身份驗證會話。

<#root>

Switch #

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 192.168.10.10
User-Name: B4-96-91-15-84-CB
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 114s
Common Session ID: 01C200650000001D62945338
Acct Session ID: 0x0000000F
Handle: 0xBE000007
Current Policy: POLICY_Gi1/0/2

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

mab Authc Success
```

步驟 4.確認Radius即時日誌

在ISE GUI中導航到**操作> RADIUS >即時日誌**，確認MAB身份驗證的即時日誌。

	Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
	0	0	0	1	0

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network De...
				Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network Device
Feb 25, 2024 04:32:06.437 PM			0	B4:96:91:15:84:CB	B4:96:91:15:84:CB	Intel-Device	C1000_MAB >> MAB_authentication	C1000_MAB >> MAB_authorizati...	PermitAccess	192.168.10.10	
Feb 25, 2024 04:32:05.396 PM				B4:96:91:15:84:CB	B4:96:91:15:84:CB	Intel-Device	C1000_MAB >> MAB_authentication	C1000_MAB >> MAB_authorizati...	PermitAccess	192.168.10.10	C1000

步驟 5.確認IP裝置跟蹤的資料包詳細資訊

運行show interfaces GigabitEthernet1/0/2命令以確認GigabitEthernet1/0/2的MAC地址。

<#root>

Switch #

show interfaces GigabitEthernet1/0/2

```
GigabitEthernet1/0/2 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 3c41.0e4f.1782 (bia 3c41.0e4f.1782)
```

在資料包捕獲中，確認ARP探測是每30秒由GigabitEthernet1/0/2傳送一次。

74 01:26:01.357866	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60 Who has 192.168.10.10? Tell 0.0.0.0
75 01:26:01.357988	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb
113 01:26:30.825787	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60 Who has 192.168.10.10? Tell 0.0.0.0
114 01:26:30.825919	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb
138 01:26:59.688695	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60 Who has 192.168.10.10? Tell 0.0.0.0
139 01:26:59.688876	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb
158 01:27:28.392691	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60 Who has 192.168.10.10? Tell 0.0.0.0
159 01:27:28.392910	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb
179 01:27:57.827636	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60 Who has 192.168.10.10? Tell 0.0.0.0
180 01:27:57.827784	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb

ARP探測

在資料包捕獲中，確認ARP探測的傳送方IP地址為0.0.0.0。

Wireshark · Packet 74 · pciPassthru0

```
> Frame 74: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
∨ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82)
    Sender IP address: 0.0.0.0
    Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
    Target IP address: 192.168.10.10
```

ARP探測的詳細資訊

問題

Catalyst交換機的IP裝置跟蹤功能可能會在傳送傳送方IP地址為0.0.0.0的ARP探測時，導致Windows PC上的IP地址衝突。

可能的解決方案

有關可能的解決方案，請參閱對重複IP地址0.0.0.0的錯誤消息進行故障排除。
以下是已在思科實驗室測試的每種解決方案的示例，以瞭解更多詳細資訊。

1. 延遲ARP探測的傳送

運行ip device tracking probe delay <1-120>命令以延遲來自交換機的ARP探頭的傳送。此命令不允許交換機在檢測到鏈路UP/flap時傳送探測<1-120>秒，這樣可最大程度地降低在鏈路另一端的主機檢查重複的IP地址時傳送探測的可能性。

以下是配置10s的ARP探測延遲的示例。

Switch (config)#ip device tracking probe delay 10

運行show ip device tracking all命令以確認延遲設定。

<#root>

Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30

Global IP Device Tracking Probe Delay Interval = 10

```
--------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
--------------------------------------------------------------------------------------------
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP

Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2
```

2. 配置ARP探測的自動源

運行ip device tracking probe auto-source fallback <host-ip> <mask> [override]命令以更改ARP探測的源IP地址。使用此命令，ARP探測的
IP源不是0.0.0.0，而是主機所在VLAN中的交換機虛擬介面(SVI)的IP地址，或者如果SVI未設定IP地址，則會自動計算該地址。

以下示例將<host-ip>配置為0.0.0.200。

Switch (config)#ip device tracking probe auto-source fallback 0.0.0.200 255.255.255.0 override

模式1.已配置SVI的IP

在本文檔中，由於為執行MAB身份驗證的介面(GigabitEthernet1/0/2)設定了SVI IP地址（vlan12的IP地址），因此ARP探測的源IP地址
更改為192.168.10.254。

運行show ip device tracking all命令以確認自動源的設定。

<#root>

```
Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
IP Device Tracking Probe Auto Source = Enabled
```

Probe source IP selection order: SVI,Fallback 0.0.0.200 255.255.255.0

```
--------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
--------------------------------------------------------------------------------------------
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP

Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2
```

在資料包捕獲中，確認ARP探測是每30秒由GigabitEthernet1/0/2傳送一次。

```
102 13:31:03.121397 3c:41:0e:4f:17:c1    IntelCor_15:84:cb            ARP    60 Who has 192.168.10.10? Tell 192.168.10.254
103 13:31:03.121608 IntelCor_15:84:cb    3c:41:0e:4f:17:c1            ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
123 13:31:33.006355 3c:41:0e:4f:17:c1    IntelCor_15:84:cb            ARP    60 Who has 192.168.10.10? Tell 192.168.10.254
124 13:31:33.006502 IntelCor_15:84:cb    3c:41:0e:4f:17:c1            ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
144 13:32:01.534263 3c:41:0e:4f:17:c1    IntelCor_15:84:cb            ARP    60 Who has 192.168.10.10? Tell 192.168.10.254
145 13:32:01.534377 IntelCor_15:84:cb    3c:41:0e:4f:17:c1            ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
163 13:32:30.386323 3c:41:0e:4f:17:c1    IntelCor_15:84:cb            ARP    60 Who has 192.168.10.10? Tell 192.168.10.254
164 13:32:30.386325 IntelCor_15:84:cb    3c:41:0e:4f:17:c1            ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
182 13:32:59.104148 3c:41:0e:4f:17:c1    IntelCor_15:84:cb            ARP    60 Who has 192.168.10.10? Tell 192.168.10.254
183 13:32:59.104318 IntelCor_15:84:cb    3c:41:0e:4f:17:c1            ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
```

ARP探測

在資料包捕獲中，確認ARP探測的傳送方IP地址為192.168.10.254，這是SVI (vlan 12)的IP。

```
Wireshark · Packet 102 · pciPassthru0

> Frame 102: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:c1 (3c:41:0e:4f:17:c1), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
∨ Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: 3c:41:0e:4f:17:c1 (3c:41:0e:4f:17:c1)
      Sender IP address: 192.168.10.254
      Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
      Target IP address: 192.168.10.10
```

ARP探測的詳細資訊

模式2.未配置SVI的IP

在本文檔中，由於ARP探測的目的地是192.168.10.10/24，如果未配置SVI IP地址，則源IP地址為192.168.10.200。

刪除SVI的IP地址。

Switch (config)#int vlan 12
Switch (config-if)#no ip address

運行show ip device tracking all命令以確認自動源的設定。

<#root>

Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
IP Device Tracking Probe Auto Source = Enabled

Probe source IP selection order: SVI,Fallback 0.0.0.200 255.255.255.0

```
--------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
--------------------------------------------------------------------------------
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP

Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2
```

在資料包捕獲中，確認ARP探測是每30秒由GigabitEthernet1/0/2傳送一次。

```
176 13:39:00.167788 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
177 13:39:00.167975 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
196 13:39:29.131512 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
197 13:39:29.131616 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
217 13:39:58.724683 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
218 13:39:58.724858 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
238 13:40:27.746620 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
239 13:40:27.746784 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
257 13:40:57.240571 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
258 13:40:57.240702 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
278 13:41:27.193284 3c:41:0e:4f:17:82    IntelCor_15:84:cb              ARP    60 Who has 192.168.10.10? Tell 192.168.10.200
279 13:41:27.193419 IntelCor_15:84:cb    3c:41:0e:4f:17:82              ARP    60 192.168.10.10 is at b4:96:91:15:84:cb
```

ARP探測

在資料包捕獲中，確認ARP探測的傳送方IP地址已更改為192.168.10.200。

```
Wireshark · Packet 176 · pciPassthru0

> Frame 176: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82)
    Sender IP address: 192.168.10.200
    Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
    Target IP address: 192.168.10.10
```

ARP探測的詳細資訊

3. 強制停用IP裝置跟蹤

運行 **ip device tracking maximum 0** 命令以停用IP裝置跟蹤。

注意：此命令並不是真正停用IP裝置跟蹤，而是將跟蹤的主機數量限制為零。

Switch (config)#int g1/0/2
Switch (config-if)#ip device tracking maximum 0

運行show ip device tracking all命令以確認GigabitEthernet1/0/2上IP裝置跟蹤的狀態。

Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled

Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0

IP Address MAC Address Vlan Interface Probe-Timeout State Source
----

Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2

參考

[排除重複IP地址0.0.0.0錯誤消息故障](#)

[驗證IPDT裝置操作](#)