排除Cisco 9800 WLC上的DHCP客戶端連線故障

目錄

簡介

本檔案將說明無線使用者端連線到Cisco 9800無線LAN控制器(WLC)時遇到的各種動態主機設定通訊協定(DHCP)相關問題以及如何進行疑難排解。

必要條件

思科建議您瞭解以下主題：

- Cisco WLC 9800的基本知識
- DHCP流的基礎知識
- 本地和Flex連線模式AP的基本知識

瞭解使用無線客戶端的DHCP流量流

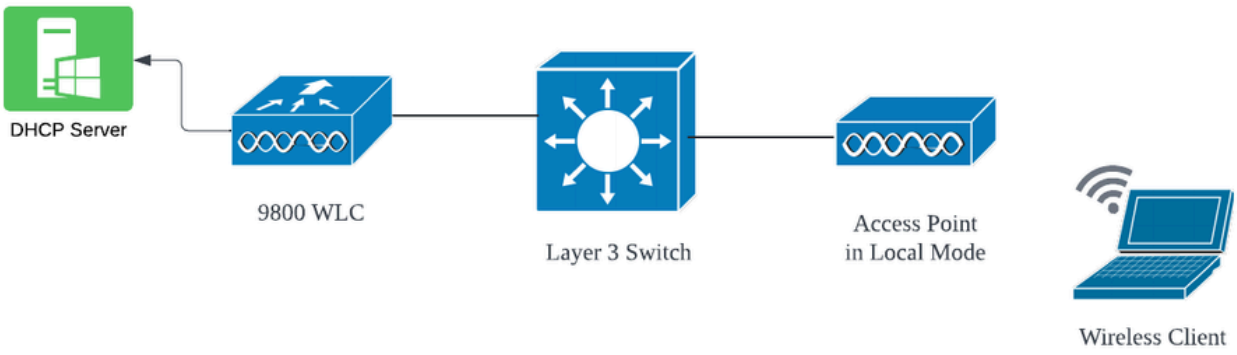
當無線客戶端連線時，它透過傳送廣播DHCP發現幀來向關聯的AP查詢DHCP伺服器，從而執行通常的DHCP交換。根據AP的運行模式，它將透過CAPWAP隧道將請求轉發到WLC或者直接將其傳遞到下一跳。如果DHCP伺服器在本地第2層域中可用，它將做出響應，從而促進連線成功。如果沒有本地子網DHCP伺服器，則必須設定路由器（使用客戶端的SVI進行配置）以將DHCP發現路由到相應的伺服器。這通常透過在路由器上配置IP幫助地址來實現，該地址指示路由器將特定的廣播UDP流量（例如DHCP請求）轉發到預定的IP地址。

客戶端DHCP流量的行為完全取決於存取點(AP)的運行模式。讓我們分別檢查這些場景：

案例 1.存取點(AP)以本地模式運行

在Local Mode下設定AP時，客戶端DHCP流量會集中交換，這意味著客戶端的DHCP請求透過CAPWAP隧道從AP傳送到WLC，然後進行相應的處理和轉發。在這種情況下，有兩種選擇：您可以使用內部DHCP伺服器，也可以選擇外部DHCP伺服器。

拓撲（本地模式AP）



網路拓撲：本地模式*AP*

案例研究1.當WLC配置為內部DHCP伺服器時

控制器能夠透過Cisco IOS XE軟體的整合功能提供內部DHCP伺服器。但是，使用外部DHCP伺服器被認為是最佳做法。在將WLC設定為內部DHCP伺服器之前，必須滿足以下幾個前提條件：

- 確保為客戶端VLAN配置交換虛擬介面(SVI)，並為其分配DHCP伺服器的IP地址。
- 內部DHCP伺服器的IP地址應在面向伺服器的介面上設定，該介面可以是環回介面、SVI或第

3層物理介面。

- 建議配置環回介面，因為與連線到實際網段的物理介面不同，環回介面不與硬體繫結，也不與裝置上的物理埠對應。環回介面的主要用途是提供一個穩定、始終開啟的介面，不受硬體故障或物理斷開的影響。

工作設定：以下是使用者端成功接收IP位址的內部DHCP伺服器組態範例。以下是操作日誌和相關設定詳細資訊。

將WLC設定為VLAN 10的DHCP伺服器，DHCP作用域範圍從10.106.10.11/24到10.106.10.50/24。

```
WLC#show run | sec dhcp
ip dhcp excluded-address 10.106.10.0 10.106.10.10
ip dhcp excluded-address 10.106.10.51 10.106.10.255
ip dhcp pool vlan_10_Pool
network 10.106.10.0 255.255.255.0
lease 0 8
```

在WLC上配置了環回介面：

```
WLC#show run interface loopback 0
interface Loopback0
ip address 10.10.10.25 255.255.255.0
end
```

將客戶端VLAN配置為SVI [L3介面]，並將幫助程式地址作為WLC上的環回介面：

<#root>

```
WLC#show run int vlan10
ip address 10.106.10.10 255.255.255.0
ip helper-address 10.10.10.25 [helper address can be loopback interface, Wireless management interface
end
```

或者，您可以在策略配置檔案內設定DHCP伺服器的IP地址，而不是在SVI下配置幫助地址。但是，為了獲得最佳實踐，通常建議對每個VLAN進行配置：

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
ipv4 dhcp server $WMI_IP
```

WLC上的放射性痕跡：

```
2024/03/29 13:28:06.502389611 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:06.502515811 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:06.502614149 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:06.502674118 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.505719129 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.505787349 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.505834315 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543149257 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:08.543254480 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.543334850 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543407760 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543910482 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543968250 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.544135443 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.544314185 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

WLC上的嵌入式資料包捕獲：

```
1401 18:58:06.501972 0.0.0.0          255.255.255.255    DHCP    348 DHCP Discover - Transaction ID 0x7030bf99
1402 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1403 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1429 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1430 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1431 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    346 DHCP Offer    - Transaction ID 0x7030bf99
1432 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    416 DHCP Offer    - Transaction ID 0x7030bf99
1433 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    452 DHCP Request  - Transaction ID 0x7030bf99
1434 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    374 DHCP Request  - Transaction ID 0x7030bf99
1435 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1436 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1437 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1438 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1439 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    346 DHCP ACK      - Transaction ID 0x7030bf99
1440 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    416 DHCP ACK      - Transaction ID 0x7030bf99
```

WLC上的嵌入式資料包捕獲

AP客戶端調試：

```
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7183] [1711718885:718317] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7184] [1711718885:718428] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7223] [1711718887:722360] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7224] chatter: dhcp_reply_nonat: 1711718887.722379604: 10
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7225] [1711718887:722524] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7591] [1711718887:759139] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7592] [1711718887:759248] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7606] [1711718887:760687] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7607] [1711718887:760780] [AP_NAME] [Client_MAC] <apr0v2>
```

客戶端資料包捕獲：

```
122 07:11:56.202853  0.0.0.0          255.255.255.255  DHCP  344 DHCP Discover - Transaction ID 0x595044d4
129 07:11:58.217331  10.106.10.10     255.255.255.255  DHCP  342 DHCP Offer    - Transaction ID 0x595044d4
130 07:11:58.219406  0.0.0.0          255.255.255.255  DHCP  370 DHCP Request  - Transaction ID 0x595044d4
131 07:11:58.227525  10.106.10.10     255.255.255.255  DHCP  342 DHCP ACK      - Transaction ID 0x595044d4
```

客戶端資料包捕獲

在所提供的操作日誌中，您可以看到WLC正在從無線客戶端接收DHCP發現消息，並且客戶端的VLAN正在將其中繼到幫助程式地址（在所提供的示例中，該地址是內部環回介面）。然後，內部伺服器發出DHCP Offer，然後客戶端傳送DHCP請求，然後伺服器使用DHCP ACK確認該請求。

驗證無線客戶端IP：

在WLC上：

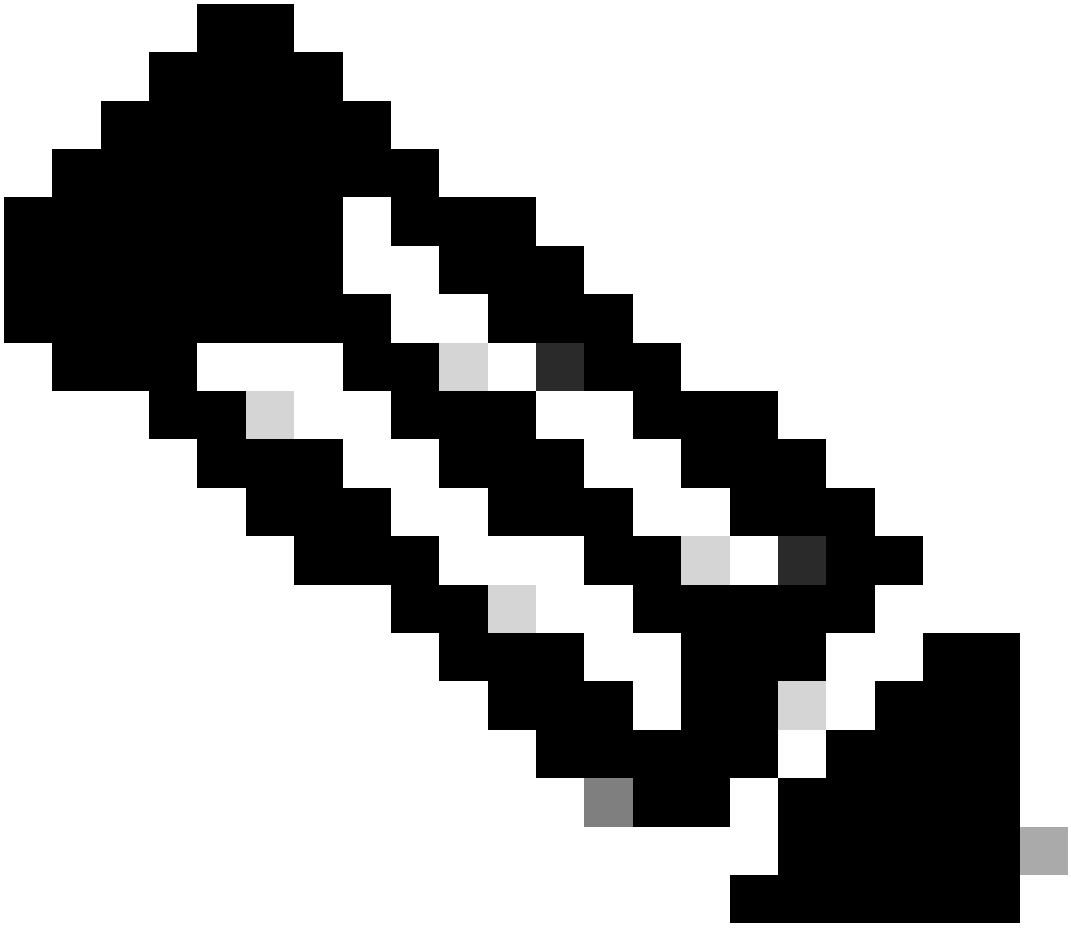
```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type          State
10.106.10.12      aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active     L
```

在無線使用者端上：

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : [redacted]
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 10.106.10.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 28, 2024 9:35:20 PM
   Lease Expires . . . . . . . . . . : Friday, March 29, 2024 6:36:29 AM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 10.10.10.25
   DHCPv6 IAID . . . . . . . . . . . : 80754501
   DHCPv6 Client DUID. . . . . . . . : [redacted]
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

使用者端上的*IP*驗證



附註：
1. 內部DHCP伺服器不支援VRF。
2. 內部DHCP伺服器不支援DHCPv6。
3. 在C9800上，SVI允許配置多個幫助程式地址，但僅使用前2個。
4. 這已經過測試，因此所有平台都支援該功能，最多佔該機箱最大客戶規模的20%。例如，對於支援64,000個客戶端的9800-80，支援的最大DHCP繫結數約為14,000。

案例分析2.使用外部DHCP伺服器時

外部DHCP伺服器是指未整合到WLC本身中，但配置在不同的網路裝置[防火牆、路由器]或網路基礎設施內的獨立實體上的DHCP伺服器。此伺服器專門用於管理IP地址和其他網路配置引數向網路上的客戶端的動態分配。

使用外部DHCP伺服器時，WLC的功能僅僅是接收和中繼流量。DHCP流量如何從WLC路由（無論是廣播還是單播）取決於您的首選項。讓我們分別考慮這些方法。

第2層域中的DHCP流量廣播

在此設定中，其他網路裝置（例如防火牆、上行鏈路或核心交換機）充當中繼代理。當客戶端廣播DHCP發現請求時，WLC的唯一工作是透過第2層介面轉發此廣播。要正確執行此操作，必須確保客戶端VLAN的第2層介面配置正確並允許其透過WLC的資料埠和上行鏈路裝置。

此例項客戶端VLAN 20的WLC端所需配置：

在WLC上配置的第2層VLAN：

```
WLC#show run vlan 20
vlan 20
name Client_vlan
end
```

已配置WLC上的資料埠以允許客戶端VLAN的流量：

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

9800 WLC上的放射性痕跡：

```
2024/03/30 10:40:43.114800606 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.114863170 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.121515725 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.121583319 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.132967882 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: IPv6 DHCP from intf
2024/03/30 10:40:43.132999148 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: IPv6 DHCP from intf
2024/03/30 10:40:43.146521529 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 10:40:43.146605773 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.146685159 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149359205 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.149419477 {wncd_x_R0-0}{1}: [client-orch-sm] [23608]: (ERR): MAC: DHCP_Server_MAC V
2024/03/30 10:40:43.149534985 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149685174 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

在9800 WLC上進行的嵌入式資料包捕獲：

```
187 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     424 DHCP Discover - Transaction ID 0xa1a4f5eb
188 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
189 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
190 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
192 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
193 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
194 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
195 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     416 DHCP Offer    - Transaction ID 0xa1a4f5eb
201 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     452 DHCP Request  - Transaction ID 0xa1a4f5eb
202 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
203 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
204 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
205 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
206 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
207 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
208 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     416 DHCP ACK      - Transaction ID 0xa1a4f5eb
```

*WLC*上的嵌入式資料包捕獲

AP客戶端調試：

```
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3650] [1711796737:183177] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3651] [1711796737:184281] [[AP_NAME] [Client_MAC] <wired0
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] [1711796737:185404 [[AP_NAME] [Client_MAC] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] chatter: dhcp_reply_nonat: 1711796737.459745189: 10
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3670] [1711796737:195085] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3683] [1711796737:368344] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3684] [1711796737:368439] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3931] [1711796737:393131] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3932] [1711796737:393250] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.4597] [1711796737:459726] [AP_Name] [Client_Mac] <wired0>
```

客戶端捕獲：

```
  3 03:17:46.193239 0.0.0.0          255.255.255.255      DHCP     342 DHCP Discover - Transaction ID 0x56883262
 31 03:17:50.649855 0.0.0.0          255.255.255.255      DHCP     342 DHCP Discover - Transaction ID 0x56883262
 34 03:17:53.259282 10.106.20.10     255.255.255.255      DHCP     342 DHCP Offer    - Transaction ID 0x56883262
 35 03:17:53.259282 10.106.20.10     255.255.255.255      DHCP     342 DHCP Offer    - Transaction ID 0x56883262
 36 03:17:53.262280 0.0.0.0          255.255.255.255      DHCP     370 DHCP Request  - Transaction ID 0x56883262
 37 03:17:53.273130 10.106.20.10     255.255.255.255      DHCP     342 DHCP ACK      - Transaction ID 0x56883262
```

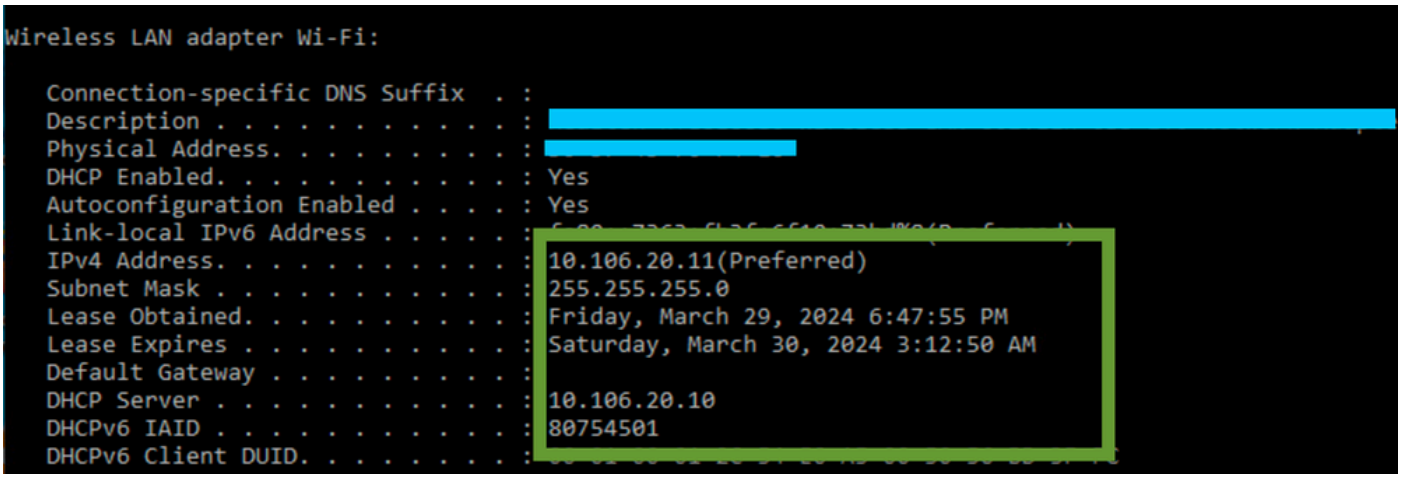
客戶端資料包捕獲

在提供的操作日誌中，您注意到WLC正在截獲來自無線客戶端的DHCP發現廣播，然後透過其第二層介面將其廣播到下一跳。WLC從伺服器收到DHCP Offer後，立即將此消息轉發到客戶端，然後傳送DHCP請求和ACK。

驗證無線客戶端IP：

您可以檢查DHCP伺服器上的IP租用及其相應的狀態。

在無線使用者端上：



使用者端上的*IP*驗證

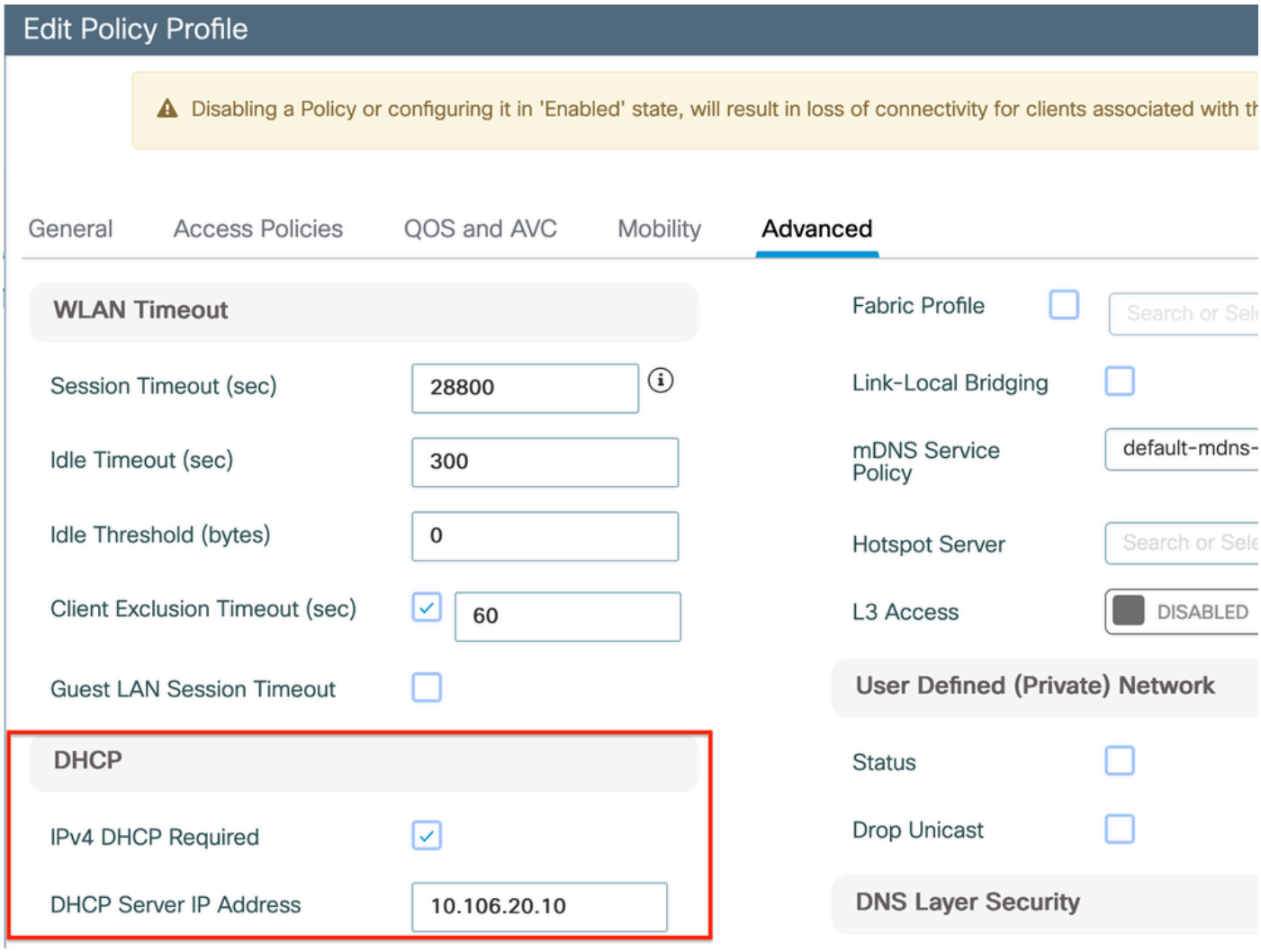
9800 WLC充當中繼代理

在此組態中，WLC會透過單點傳播，直接將從無線使用者端接收的DHCP封包轉送到DHCP伺服器。要啟用此功能，請確保在WLC上配置了客戶端的VLAN SVI。

在9800 WLC中配置DHCP伺服器IP的方法有兩種：

1. 在「高級設定」下的「策略配置檔案」下配置DHCP伺服器IP。

透過GUI：導航到Configuration > Tags & Profile > Policy > Policy_name > Advanced. 在DHCP部分下，您可以配置DHCP伺服器IP，如下所示：



WLC上的策略配置檔案設定

透過CLI：

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
ipv4 dhcp server $DHCP_Server_IP
```

2. 在SVI配置中，您必須指定幫助程式地址。可以在幫助地址配置中設定多個DHCP伺服器以提供冗餘。雖然可以為策略配置檔案中的每個WLAN設定DHCP伺服器地址，但推薦的方法是按介面進行配置。這可以透過為相應的SVI分配幫助地址來實現。

採用中繼功能時，DHCP流量的來源將是客戶端的交換虛擬介面(SVI)的IP地址。然後，透過路由表確定的與目標（DHCP伺服器的IP地址）對應的介面路由此流量。

以下是9800作為中繼代理的工作配置示例：

使用幫助程式地址為WLC上的客戶端VLAN配置第3層介面：

```
WLC#show run int vlan 20
interface vlan 20
```

```
ip address 10.106.20.1 255.255.255.0
ip helper-address 10.106.20.10
end
```

已配置WLC上的資料埠以允許客戶端VLAN的流量：

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

來自WLC的RA跟蹤：

```
2024/03/30 13:46:38.549504590 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:38.549611716 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:38.549666984 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.597696305 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.597778465 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.597829829 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.598444184 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.598506350 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.598544420 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.621660873 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 13:46:41.621771405 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.621851320 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.621908730 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625257607 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.625329089 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.625490562 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625655045 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

WLC上的嵌入式資料包捕獲：

No.	Time	Source	Destination	Protocol	Lengtr	Info
462	19:16:34.544969	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
463	19:16:34.545961	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
594	19:16:38.548967	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
595	19:16:38.548967	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
647	19:16:41.596953	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
648	19:16:41.596953	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
649	19:16:41.597961	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
650	19:16:41.597961	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
653	19:16:41.620954	0.0.0.0	255.255.255.255	DHCP	452	DHCP Request - Transaction ID 0x137ea7ac
654	19:16:41.620954	10.106.20.1	10.106.20.10	DHCP	374	DHCP Request - Transaction ID 0x137ea7ac
655	19:16:41.624967	10.106.20.10	10.106.20.1	DHCP	346	DHCP ACK - Transaction ID 0x137ea7ac
656	19:16:41.624967	10.106.20.1	255.255.255.255	DHCP	416	DHCP ACK - Transaction ID 0x137ea7ac

WLC上的嵌入式資料包捕獲

在WLC上的放射性跟蹤(RA)和嵌入式資料包捕獲(EPC)中，您會發現WLC作為中繼代理，正在將DHCP資料包直接從客戶端傳送到DHCP伺服器。

AP客戶端調試：

```
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7476] [1711806397:747677] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7481] [1711806397:748177] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] chatter: dhcp_reply_nonat: 1711806400.797214204: 10
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] [1711806400:797362] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7978] [1711806400:797870] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7979] [1711806400:797903] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8204] [1711806400:820455] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8205] [1711806400:820550] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8248] [1711806400:824829] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8249] [1711806400:824911] [AP_Name] [Client_MAC] <apr0v1>
```

客戶端捕獲：

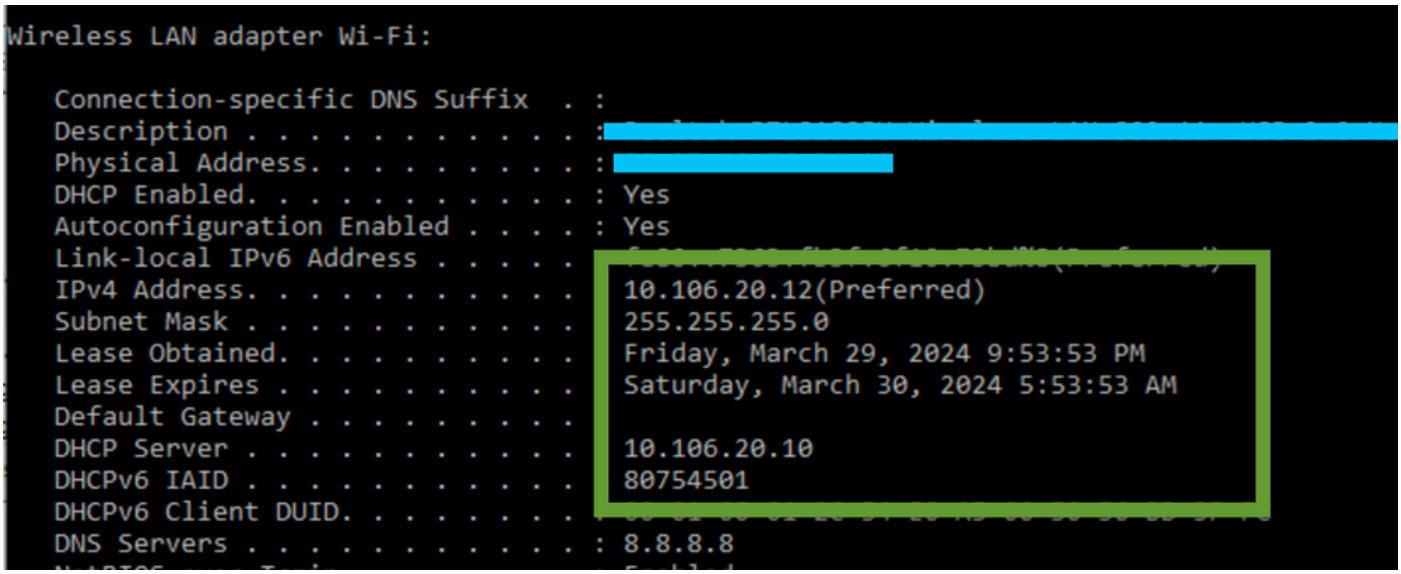
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
60	10:23:53.696530	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x137ea7ac
61	10:23:53.698634	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
62	10:23:53.737816	10.106.20.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x137ea7ac

客戶端資料包捕獲

驗證無線客戶端IP：

您可以檢查DHCP伺服器上的IP租用及其相應的狀態。

在無線使用者端上：



使用者端上的IP驗證

9800 WLC中的DHCP選項80及子選項5/150

在某些場景中，您可能更願意明確定義DHCP流量的源介面，而不是根據路由表來定義，以防止潛在的網路複雜性。當路徑上的下一個網路裝置（例如第3層交換機或防火牆）採用反向路徑轉發(RPF)檢查時，這一點尤其重要。例如，無線管理介面在VLAN 50上設定，而客戶端SVI在VLAN 20上並用作客戶端流量的DHCP中繼。預設路由定向到無線管理VLAN/子網的網關。

從9800 WLC上的版本17.03.03開始，可以為DHCP流量選擇源介面，作為客戶端VLAN或另一個VLAN，例如無線管理介面

(WMI)，保證與DHCP伺服器的連線。

以下是組態片段：

```
!
interface vlan 50
 description Wireless Management
 ip address 10.100.16.10 255.255.255.0
!
interface vlan 20
 description Wireless_Client_vlan
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
!
ip route 0.0.0.0 0.0.0.0 10.100.16.1
```

在此場景中，到DHCP伺服器10.100.17.14的流量將源自VLAN 50 (10.100.16.10)，因為資料包的送出介面是基於IP路由表中的查詢選擇的，並且由於配置了預設路由，通常它將透過無線管理介面(WMI) VLAN送出。
但是，如果上行鏈路交換機實施反向路徑轉發(RPF)檢查，則它可能會丟棄來自VLAN 50、但IP源地址屬於不同子網[VLAN 20]的資料包。

要防止出現這種情況，您應該使用IP DHCP relay source-interface命令為DHCP資料包設定精確的源介面。在這種情況下，您會希望DHCP資料包從VLAN 50上的WMI介面發出：

```
interface vlan 20
 description Wireless_Client_vlan=
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
 ip dhcp relay source-interface vlan 50
```

使用ip dhcp relay source-interface命令時，DHCP資料包的源介面和GIADDR都設定為在DHCP中繼命令中指定的介面（本例中為VLAN50）。這是一個問題，因為這不是要分配DHCP地址的客戶端VLAN。

DHCP伺服器如何知道如何從正確的客戶端池分配IP？

因此，當使用ip dhcp relay source-interface 命令時，C9800會自動將客戶端子網資訊增加到選項82的專有子選項150（稱為鏈路選擇），如您在捕獲資訊中所見：

```
Relay agent IP address: 10.100.16.10
Client MAC address: [redacted]
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
v Option: (82) Agent Information Option
    Length: 6
  v Option 82 Suboption: (150) Link selection (Cisco proprietary) (192.168.4.2)
      Length: 4
      Link selection (Cisco proprietary): 192.168.4.2
```

WLC資料包捕獲上的選項182子選項150

預設情況下，它將增加子選項150（思科專有）。確保使用的DHCP伺服器可以解釋這些資訊並對其執行操作。建議將C9800配置更改為使用標準選項82子選項5傳送鏈路選擇資訊。您可以透過配置以下全局命令執行此操作：

```
<#root>

C9800(config)#ip dhcp compatibility suboption link-selection standard
```

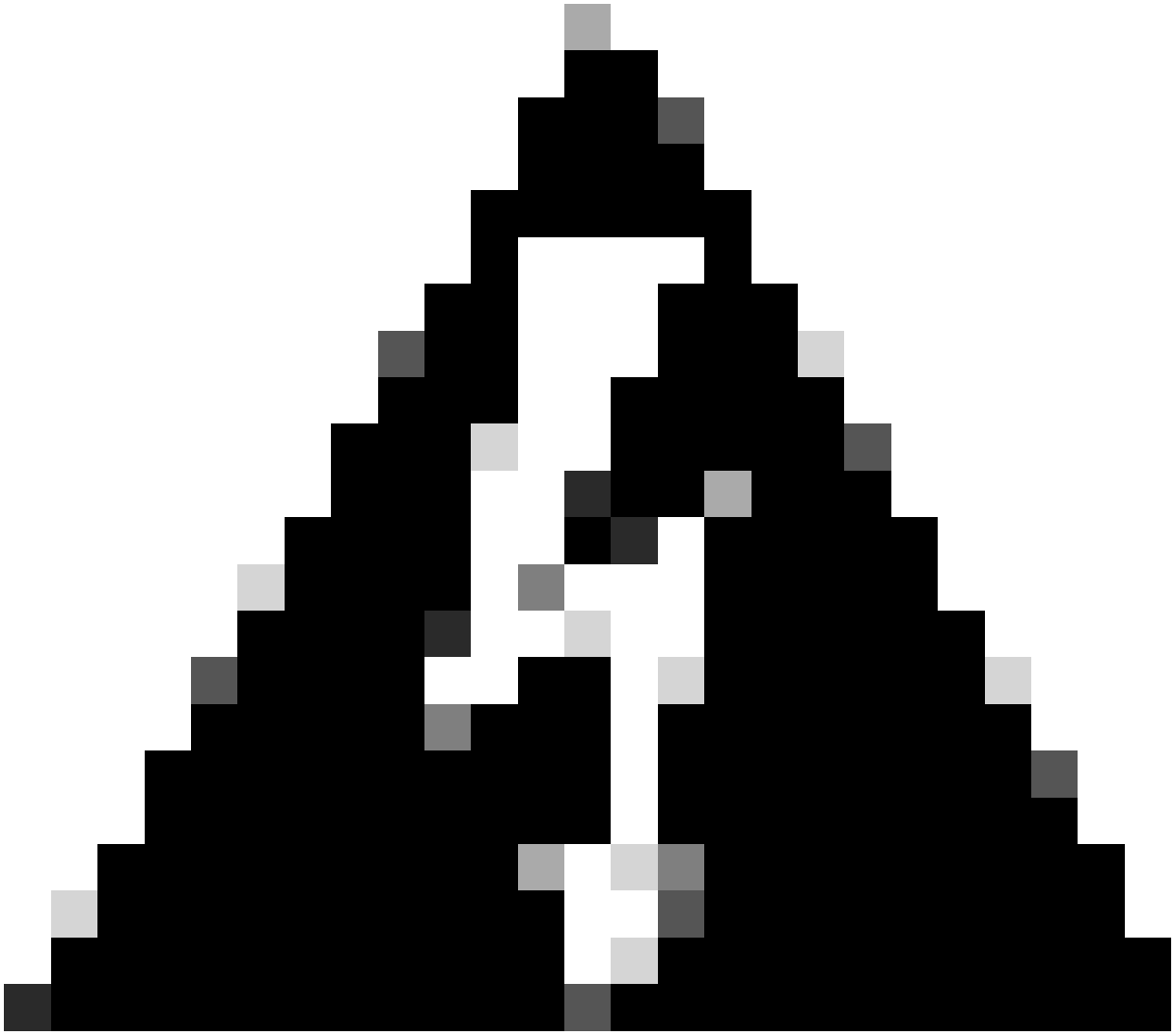
應用指定的命令後，系統將使用DHCP資料包中的子選項5替換子選項150。網路裝置可以更廣泛地辨識子選項5，從而確保資料包被丟棄的可能性更低。此變更的應用程式在所提供的擷取中也很明顯：

```
Relay agent IP address: 10.100.16.10
Client MAC address: [redacted]
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
v Option: (82) Agent Information Option
    Length: 6
  > Option 82 Suboption: (5) Link selection (192.168.4.2)
```

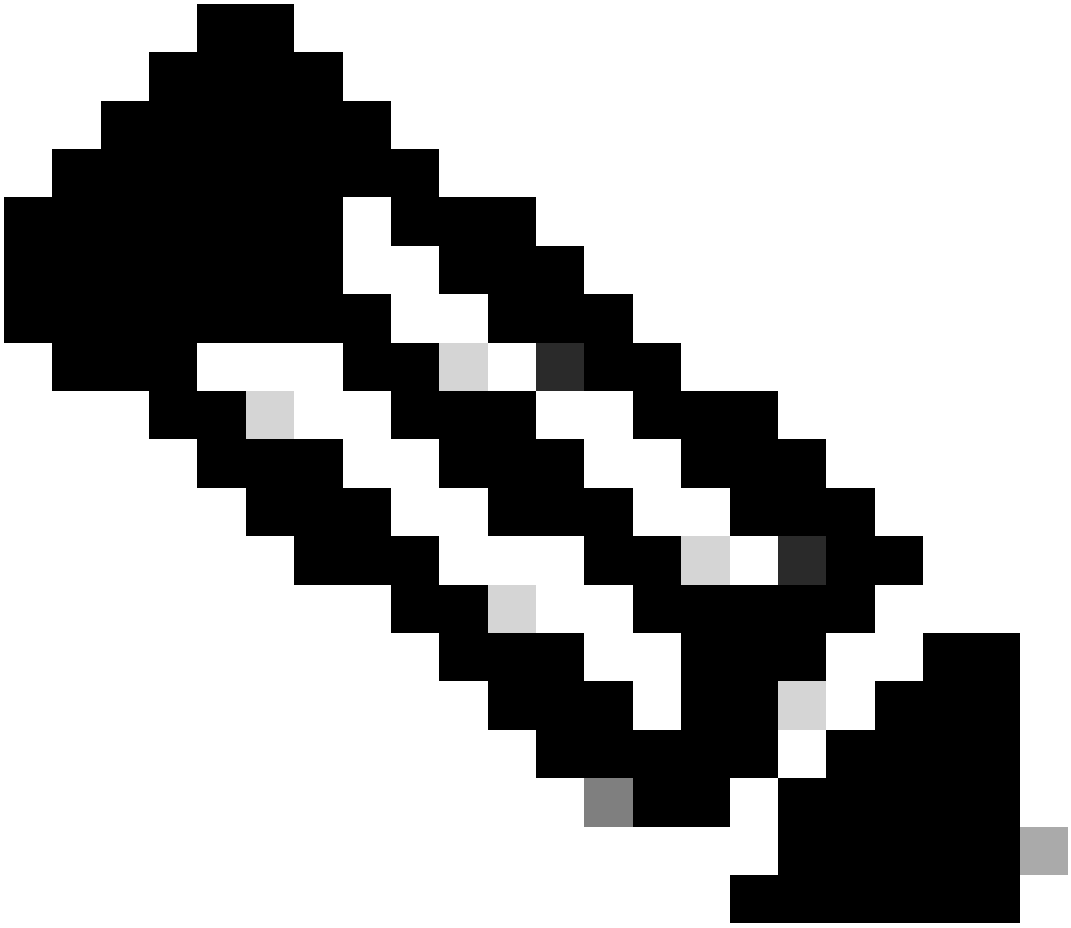
WLC資料包捕獲上的選項182子選項5

實施子選項5後，您的DHCP流量應該由其他網路裝置確認。但是，您仍可能會遇到NAK（否定確認）消息，特別是在使用Windows DHCP伺服器時。這可能是由於DHCP伺服器未授權源IP地址，可能是因為它沒有該源IP的相應配置。

您必須在DHCP伺服器上執行什麼操作？對於Windows DHCP伺服器，必須建立一個虛擬作用域來授權中繼代理的IP。



警告：所有中繼代理IP地址(GIADDR)必須是活動DHCP作用域IP地址範圍的一部分。DHCP作用域IP地址範圍之外的任何GIADDR都被視為惡意中繼，Windows DHCP伺服器不會確認來自這些中繼代理的DHCP客戶端請求。可以建立特殊作用域來授權中繼代理。使用GIADDR建立範圍（如果GIADDR是連續的IP位址，則為multiple），從分配中排除GIADDR位址，然後啟動範圍。這將授權中繼代理，同時阻止分配GIADDR地址。

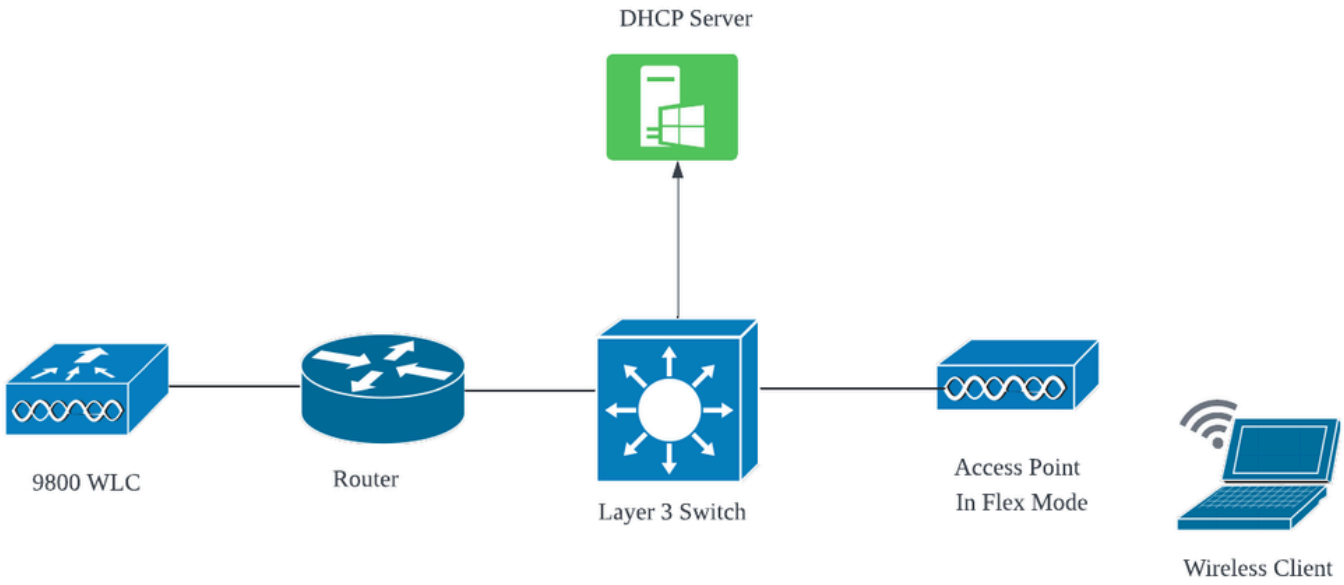


注意：在外錨點設定中，DHCP資料流透過將AP模式設定為本地模式進行集中處理。最初，DHCP請求會傳送到外部WLC，然後WLC透過移動隧道將其轉發到錨點WLC。它是根據已配置的設定處理流量的錨點WLC。因此，所有與DHCP相關的配置都應在錨點WLC上實現。

案例 2.存取點(AP)以Flex模式運行

FlexConnect AP專為分支機構和遠端辦公室設計，允許它們在失去與中央無線區域網控制器(WLC)的連線時以獨立模式運行。FlexConnect AP可以在本機交換使用者端和網路之間的流量，而不需要將流量回傳到WLC。這減少了延遲並節省了WAN頻寬。在Flex模式下，DHCP流量可以集中交換或本地交換。

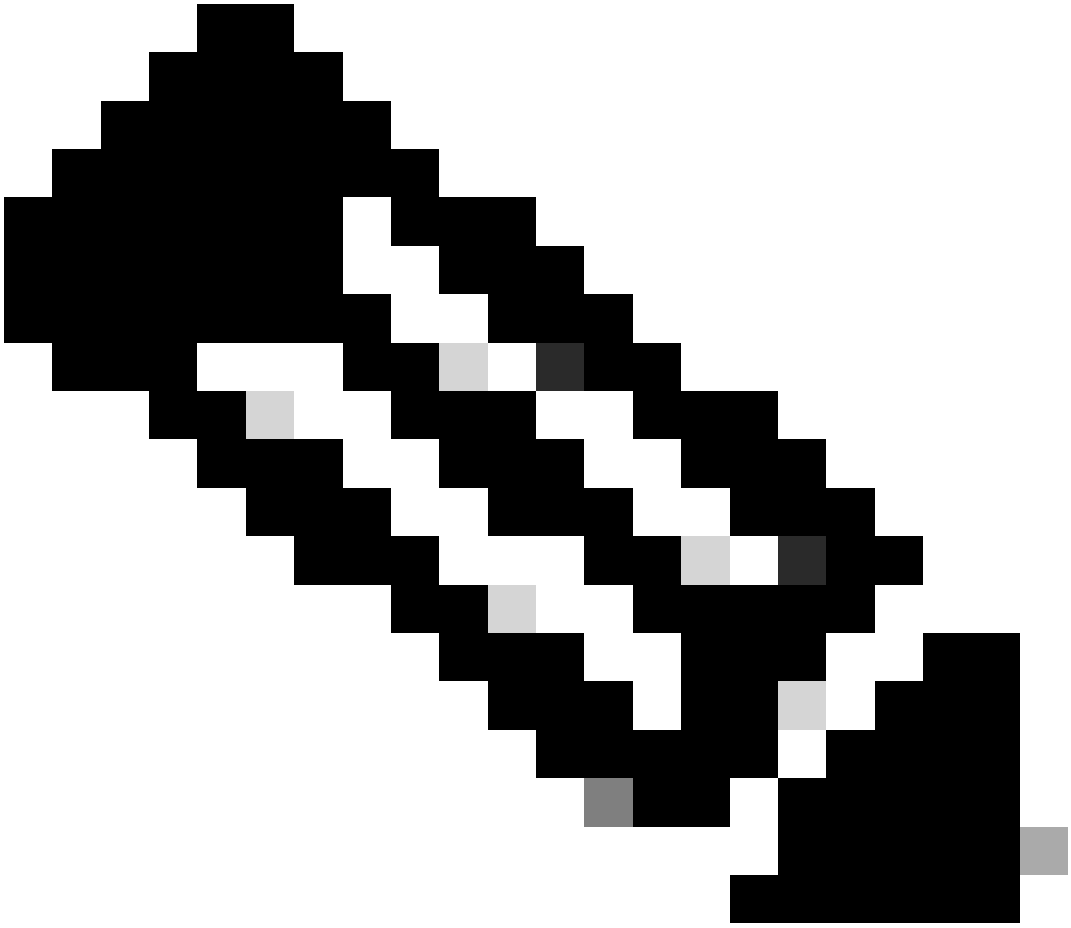
拓撲（Flex模式AP）



網路拓撲：*Flex*模式*AP*

使用中央DHCP的FlexConnect模式AP

使用中央DHCP伺服器時，無論AP模式如何，配置、操作流程和故障排除步驟都保持一致。但是，對於FlexConnect模式下的AP，通常建議使用本地DHCP伺服器，除非您在本地站點上設定客戶端SVI。



注意：如果遠端站點沒有可用的客戶端子網，則可以使用FlexConnect NAT-PAT。FlexConnect NAT/PAT對源自連線到AP的客戶端的流量執行網路地址轉換(NAT)，將其對映到AP的管理IP地址。例如，如果您的AP在遠端分支機構以FlexConnect模式運行，並且連線的客戶端需要與位於控制器所在總部的DHCP伺服器通訊，則可以結合策略配置檔案中的中央DHCP設定來啟用FlexConnect NAT/PAT。

使用本地DHCP的FlexConnect模式AP

當FlexConnect AP配置為使用本地DHCP時，與AP關聯的客戶端裝置會從同一本地網路中可用的DHCP伺服器接收其IP地址配置。此本地DHCP伺服器可以是路由器、專用DHCP伺服器，或本地子網內提供DHCP服務的任何其他網路裝置。使用本地DHCP時，DHCP流量在本地網路內交換，這意味著AP直接從客戶端將DHCP請求中繼到相鄰跳（如接入交換機）。從這裡開始，會根據您的網路組態來處理要求。

必備條件:

1. 請參閱FlexConnect指南，確保您的配置與指南中概述的說明和最佳實踐一致。

2. 客戶端VLAN應列在flex profile下。
3. 需要將AP設定為中繼模式，將AP管理VLAN指定為本地VLAN，並且中繼上應允許用於客戶端流量的VLAN。

以下是AP連線的交換機埠配置的示例，其中管理VLAN為58，客戶端VLAN為20：

```
Switch#show run int gig1/0/2
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 20,58
switchport trunk encapsulation dot1q
switchport trunk native vlan 58
switchport mode trunk
end
!
```

工作設定：針對Flex模式設定AP時，與本機DHCP伺服器共用作業記錄的參考：

AP客戶端調試：

```
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6056] [1712144373:605628] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6057] chatter: dhcp_req_local_sw_nonat: 1712144373.6056478
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] [1712144373:605830] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] chatter: dhcp_reply_nonat: 1712144373.605647862: 0.0
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.7462] [1712144376:746192] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9149] chatter: dhcp_from_inet: 1712144376.914892705: 10.10
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9150] chatter: dhcp_reply_nonat: 1712144376.914892705: 10.
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9151] [1712144376:915159] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9161] [1712144376:916101] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9373] [1712144376:937350] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9645] [1712144376:964530] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9646] chatter: dhcp_req_local_sw_nonat: 1712144376.9645492
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9647] [1712144376:964749] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] CLSM[client_mac]: client moved from IPLEARN_PENDING
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] [1712144376:973687] [AP_Name] [client_mac] <apr0v1>
```

AP上行鏈路捕獲：

```
1399 18:37:…  0.0.0.0          255.255.255.255    DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1400 18:37:…  0.0.0.0          255.255.255.255    DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1499 18:37:…  0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0xb530583d
1500 18:37:…  0.0.0.0          255.255.255.255    DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1545 18:38:…  10.106.20.10     255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0xb530583d
1546 18:38:…  10.106.20.10     255.255.255.255    DHCP    420 DHCP Offer    - Transaction ID 0xb530583d
1547 18:38:…  10.106.20.10     255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0xb530583d
1548 18:38:…  10.106.20.10     255.255.255.255    DHCP    420 DHCP Offer    - Transaction ID 0xb530583d
1553 18:38:…  0.0.0.0          255.255.255.255    DHCP    370 DHCP Request  - Transaction ID 0xb530583d
1555 18:38:…  0.0.0.0          255.255.255.255    DHCP    448 DHCP Request  - Transaction ID 0xb530583d
1556 18:38:…  10.106.20.10     255.255.255.255    DHCP    342 DHCP ACK      - Transaction ID 0xb530583d
1558 18:38:…  10.106.20.10     255.255.255.255    DHCP    420 DHCP ACK      - Transaction ID 0xb530583d
```

AP上行鏈路捕獲

客戶端捕獲：

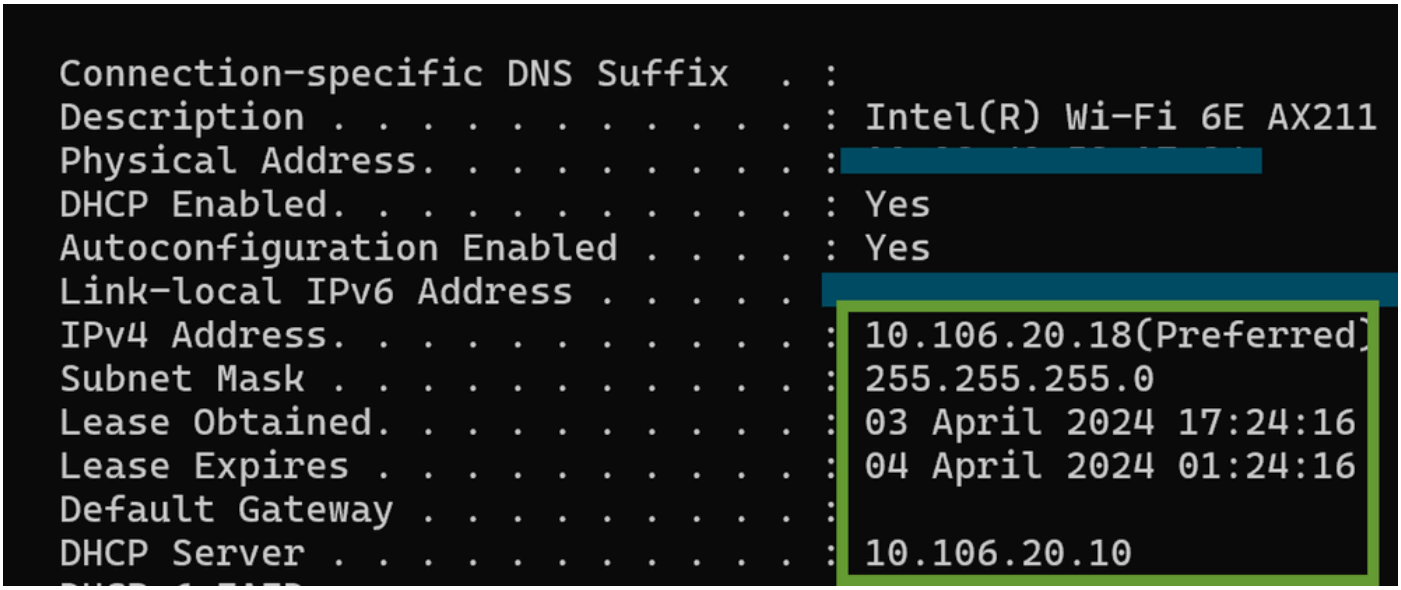
```
16540 111.905836    0.0.0.0          255.255.255.255    DHCP     343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18       DHCP     342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255    DHCP     385 DHCP Request  - Transaction ID 0x628c01b4
16543 112.304391    10.106.20.10     10.106.20.18       DHCP     342 DHCP ACK      - Transaction ID 0x628c01b4
```

客戶端資料包捕獲

驗證無線客戶端IP：

您可以檢查DHCP伺服器上的IP租用及其相應的狀態。

在無線使用者端上：



使用者端上的*IP*驗證

DHCP問題故障排除

排除DHCP故障涉及確定並解決阻止客戶端在連線到無線網路時從DHCP伺服器獲取IP地址的問題。以下是排除DHCP故障時的一些常見步驟和注意事項：

1. 驗證客戶端配置

- 確保客戶端配置為自動獲取IP地址。
- 確認網路介面卡已啟用且運作正常。

2. 檢查DHCP伺服器狀態

- 確認DHCP伺服器運行正常且可從客戶端網段訪問。
- 檢查DHCP伺服器的IP地址、子網掩碼和預設網關設定。

3. 審查範圍配置

- 檢查DHCP作用域，確保它有足夠的IP地址範圍可供客戶端使用。
- 驗證作用域的租用期限和選項，例如DNS伺服器和預設網關
- 在某些環境（如Active Directory）中，請確保DHCP伺服器有權在網路內提供DHCP服務。

4. 檢視9800 WLC上的配置

- 由於配置錯誤而出現了許多問題，例如缺少環回介面、客戶端SVI或缺少已配置的幫助地址。在收集日誌之前，建議驗證配置是否正確實施。
- 使用內部DHCP伺服器時：關於DHCP作用域的耗盡，必須確保根據您的要求配置租用計時器，特別是在透過CLI配置DHCP時。預設情況下，9800 WLC上的租用計時器設定為無限。
- 使用中央DHCP伺服器時，確認WLC上行鏈路連線埠上允許使用者端VLAN流量。相反，如果使用本地DHCP伺服器，請確保在AP上行鏈路埠上允許相關VLAN。

5. 防火牆和安全設定

- 確保防火牆或保安軟體未阻止DHCP流量（DHCP伺服器的埠67和DHCP客戶端的埠68）。

日誌收集

來自WLC的日誌

1. 啟用術語exec提示符時間戳，讓所有命令都有時間引用。

2. 使用show tech-support wireless !! 檢視配置

2. 您可以檢查從屬端數目、從屬端狀態分佈和排除的從屬端。
show wireless summary !! AP和客戶端總數
show wireless exclusionlist !! 如果任何使用者端被視為已排除
show wireless exclusionlist client mac-address MAC@ !! 獲取有關排除特定客戶端的更多詳細資訊，並檢查原因是否被列為任何客戶端的IP盜竊。

3. 檢查客戶端的IP地址分配，查詢錯誤地址或意外的靜態地址學習，VLAN標籤為已更新（由於DHCP伺服器沒有響應），或處理DHCP/ARP的SISF中的資料包丟棄。

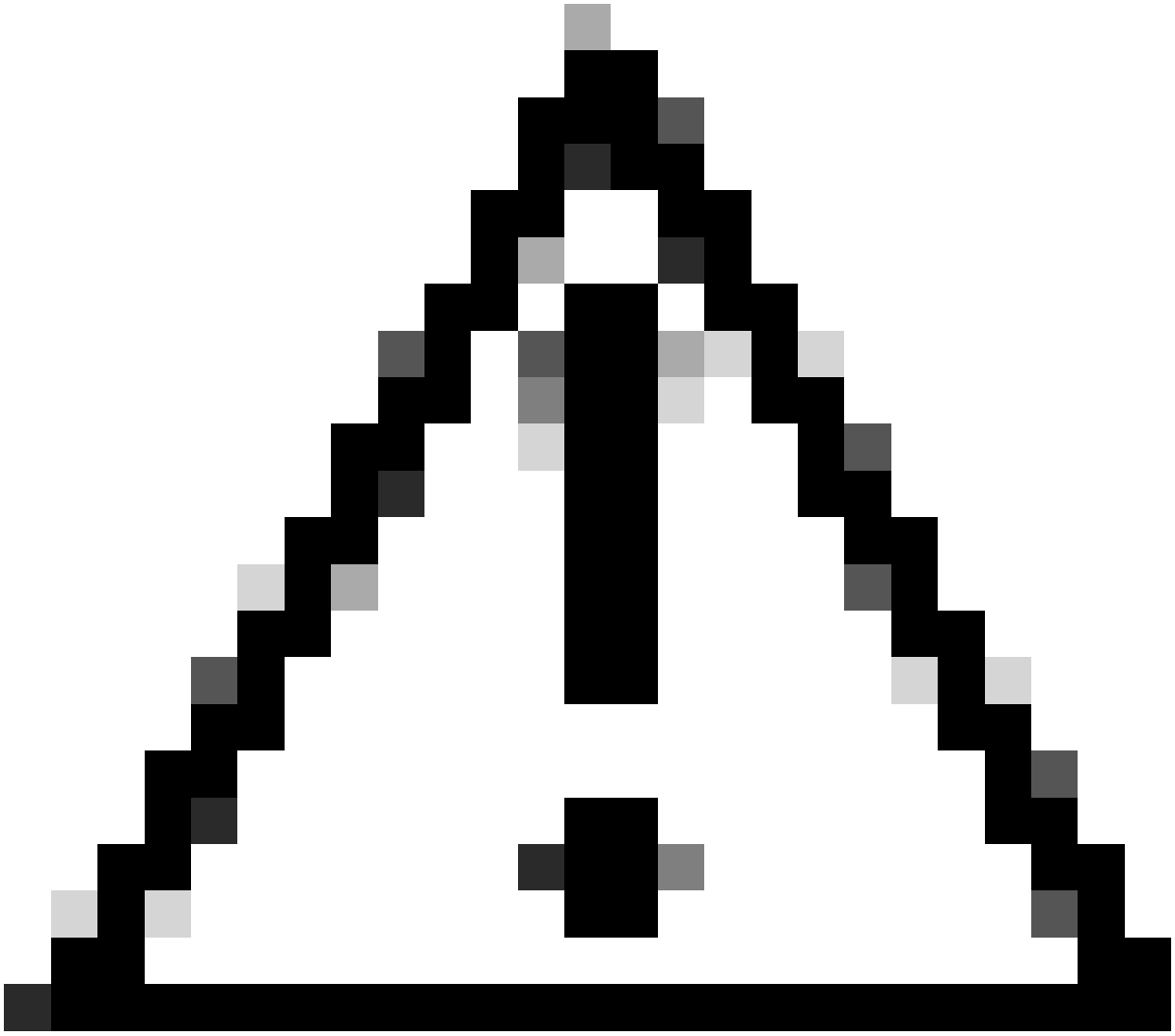
show wireless device-tracking database ip !! 按IP檢查並檢視地址學習過程：
show wireless device-tracking database mac !! 透過Mac檢查並檢視分配了哪個IP客戶端。
show wireless vlan details !! 使用VLAN群組時，請檢查VLAN是否未因DHCP失敗而標籤為已修改。
show wireless device-tracking feature drop !!SISF中的丟棄

4. WLC針對具體客戶端MAC@的特定輸出 show wireless device-tracking feature drop

當客戶端嘗試連線無線網路時，啟用客戶端MAC地址的放射性跟蹤。

透過CLI：

debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting time allows us to enable traces for up to 24 days
!!Reproduce [Clients should stuck in IP learn]
no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
dir bootflash: | i debug



注意：條件調試會啟用調試級別日誌記錄，這反過來會增加生成的日誌量。保持此運行狀態可減少從檢視日誌的時間間隔。因此，建議在故障排除會話結束時始終停用調試。

要停用所有調試，請運行以下命令：

```
# clear platform condition all
# undebug all
```

透過GUI：

步驟 1.導覽至 Troubleshooting > Radioactive Trace .

步驟 2.按一下Add，然後輸入要排除故障的客戶端Mac地址。您可以增加多個Mac地址進行跟蹤。

步驟 3.當您準備好開始放射性追蹤時，請按一下「開始」。啟動後，調試日誌記錄將寫入磁碟，記錄與跟蹤的MAC地址相關的任何控制層面處理情況。

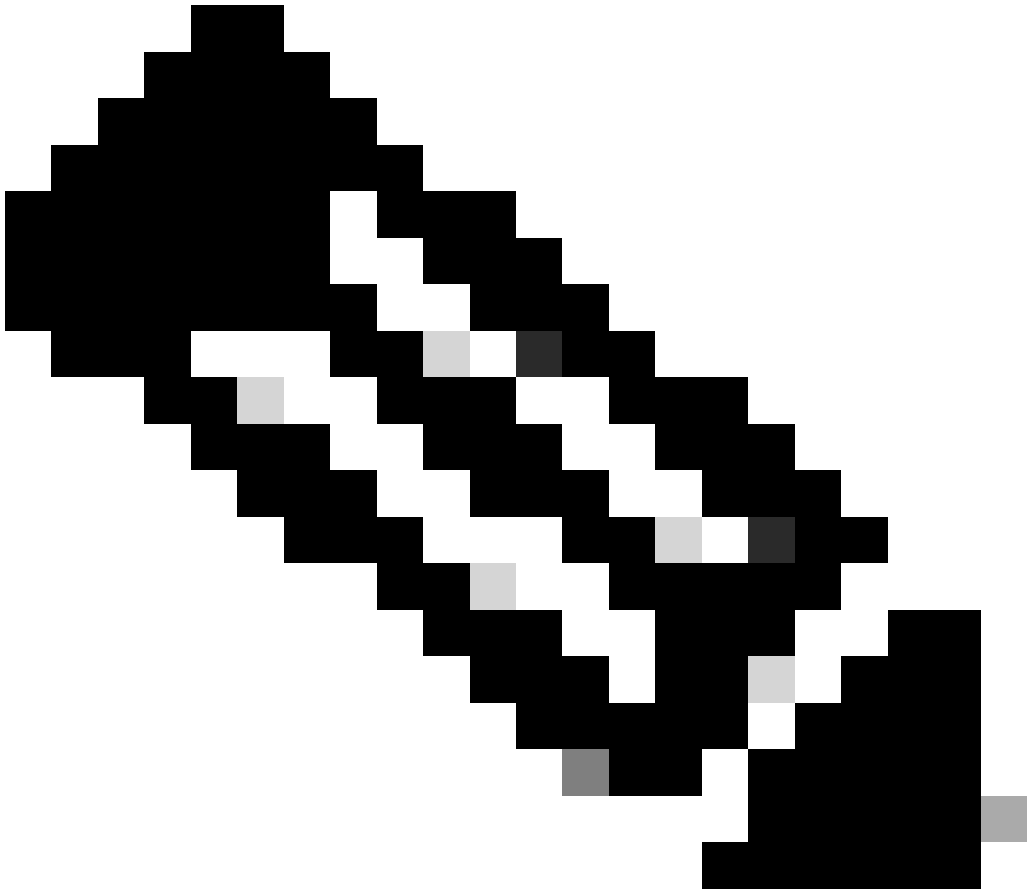
步驟 4.重現要排除故障的問題時，按一下Stop。

步驟 5.對於每個調試的mac地址，您可以透過按一下 Generate 來生成一個日誌檔案，整理屬於該mac地址的所有日誌。

步驟 6.選擇您要經過分頁的記錄檔的備份時間，然後按一下「套用至裝置」。

步驟 7.現在您可以按一下檔案名稱旁邊的小圖示來下載檔案。此檔案存在於控制器的開機快閃磁碟機中，也可以透過CLI從包裝箱中複製。

!!按客戶端MAC地址雙向過濾的嵌入式捕獲，客戶端內部MAC過濾器在17.1以後可用。



註：在9800 WLC上啟用中央DHCP時，9800上的EPC將非常有用。

透過CLI：

```
monitor capture MYCAP clear
monitor capture MYCAP interface Po1 both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!!Reproduce
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap
```

透過GUI：
步驟 1.導航到Troubleshooting > Packet Capture > +Add。

步驟 2.定義資料包捕獲的名稱。最多允許8個字元。

步驟 3.定義篩選條件（如果有）。

步驟 4.如果希望看到流量被傳送至系統CPU並注入資料平面中，請選中此框以監控控制流量。

步驟 5.定義緩衝區大小。最多允許100 MB。

步驟 6.根據需要定義允許範圍1 - 1000000秒的期限或允許範圍1 - 100000個資料包的資料包數量。

步驟 7.從左側列中的介面清單中選擇介面，並選擇箭頭將其移動到右側列。

步驟 8.儲存並應用到裝置。

步驟 9.若要開始擷取，請選取開始。

步驟 10.您可以讓擷取執行到定義的限制。要手動停止捕獲，請選擇停止。

步驟 11.停止後，可使用「導出」(Export)按鈕按一下此選項，以透過HTTP或TFTP伺服器、FTP伺服器、本地系統硬碟或快閃記憶體將捕獲檔案(.pcap)下載到本地案頭。

來自AP端的日誌

```
show tech !! Collect show tech to have all config details and client stats for the AP.
term mon
!!Basic
debug client MAC@
```

來自DHCP伺服器的日誌

使用外部DHCP伺服器時，需要在伺服器端收集調試日誌和資料包捕獲資訊，以驗證DHCP流量的流動。

其他日誌

如果您發現DHCP發現消息在中央DHCP設定中的9800 WLC上可見，或者在本地DHCP設定中的AP調試日誌中可見，則您應該繼續從上行鏈路收集捕獲資料，以確認資料包沒有丟棄到乙太網埠。根據交換機的功能，您可以選擇在上行鏈路交換機上執行嵌入式資料包捕獲或SPAN（交換埠分析器）捕獲。建議逐步跟蹤DHCP流量以確定通訊中斷的點（從DHCP客戶端到DHCP伺服器以及反向方向）。

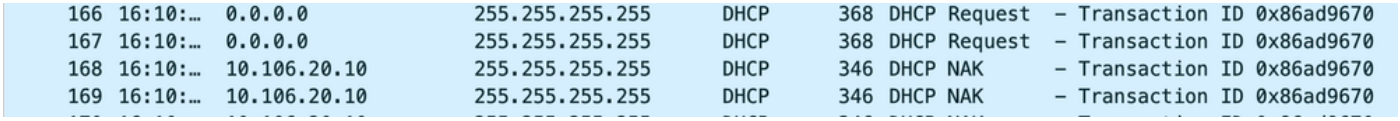
已知的問題

問題1.使用者端正在嘗試從先前保留的VLAN取得IP位址。可能會出現無線客戶端在與不同客戶端VLAN關聯的兩個SSID之間切換的情況。在這種情況下，使用者端可能會持續從先前連線的VLAN要求IP。因為此IP不在當前VLAN的DHCP作用域內，所以DHCP伺服器將發出NAK（否定確認），因此，客戶端將無法獲取IP地址。

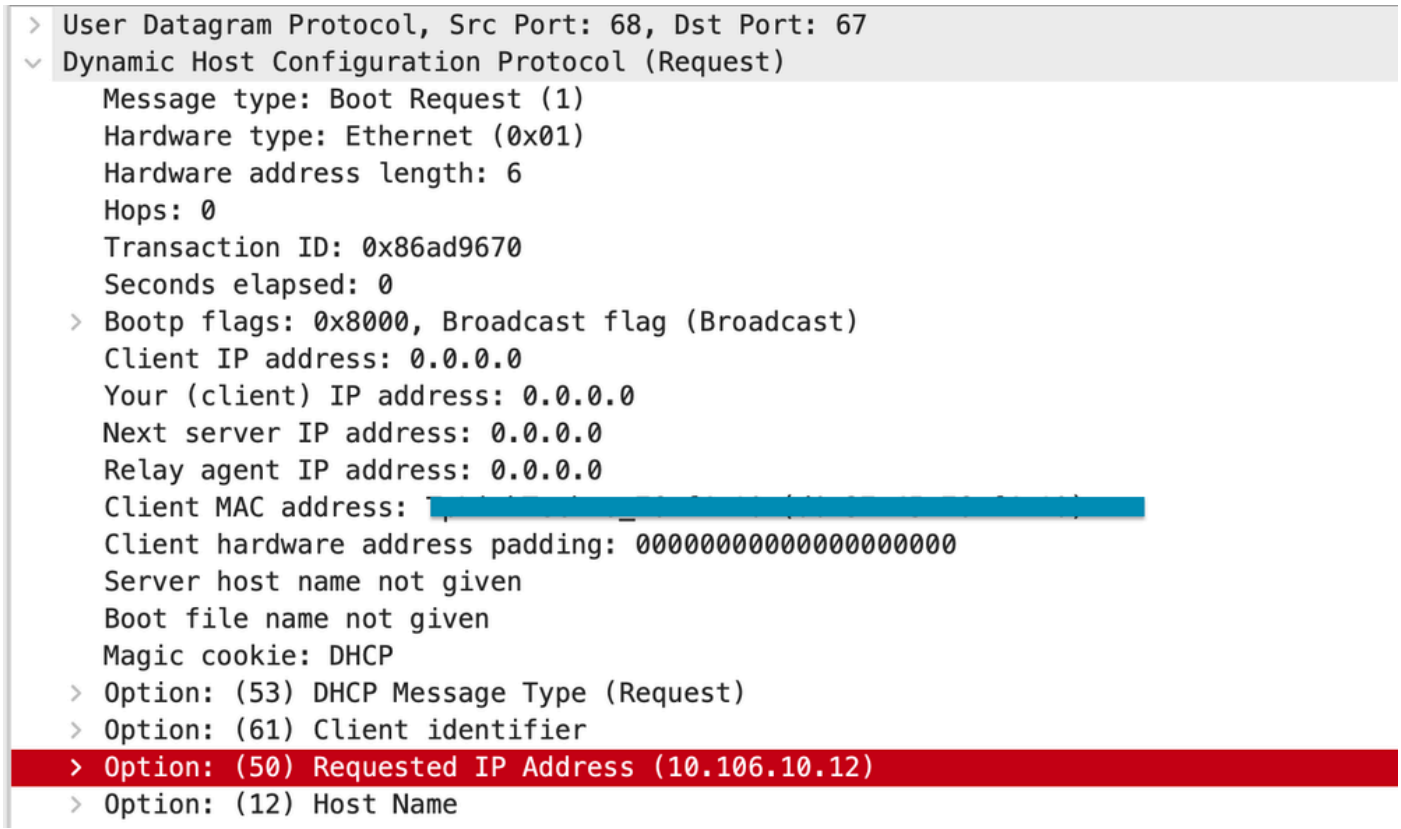
在放射跟蹤日誌中，儘管當前SSID的客戶端VLAN是VLAN 20，但客戶端仍繼續從以前連線的VLAN（即VLAN 10）中查詢IP。

```
2024/03/30 10:40:43.050956833 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.051051895 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.058538643 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.058658561 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
```

WLC上的嵌入式資料包捕獲：



WLC上的嵌入式資料包捕獲



WLC資料包捕獲上的DHCP選項50

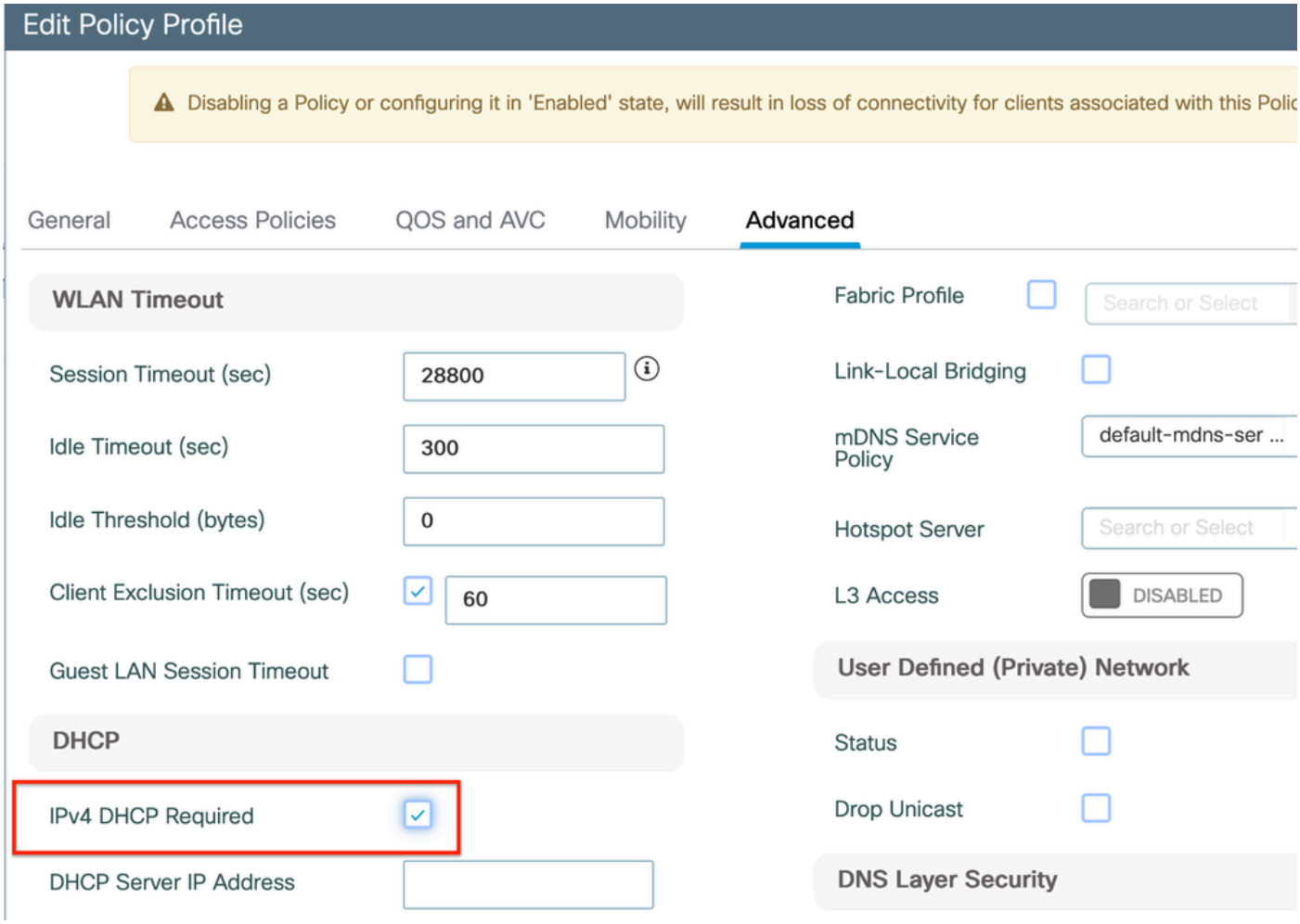
解決方案：為確保客戶端完成完整的DHCP過程，可以在策略配置中啟用IPv4 DHCP Required選項。應啟用此設定，尤其是當客戶端在SSID之間切換時，允許DHCP伺服器從與先前SSID關聯的VLAN請求IP地址時向客戶端傳送NAK。否則，客戶端可能會繼續使用或請求其先前持有的IP地址，從而導致通訊中斷。但是，請注意，啟用此功能將影響配置了靜態IP地址的無線客戶端。

以下為啟用所需選項的流程：

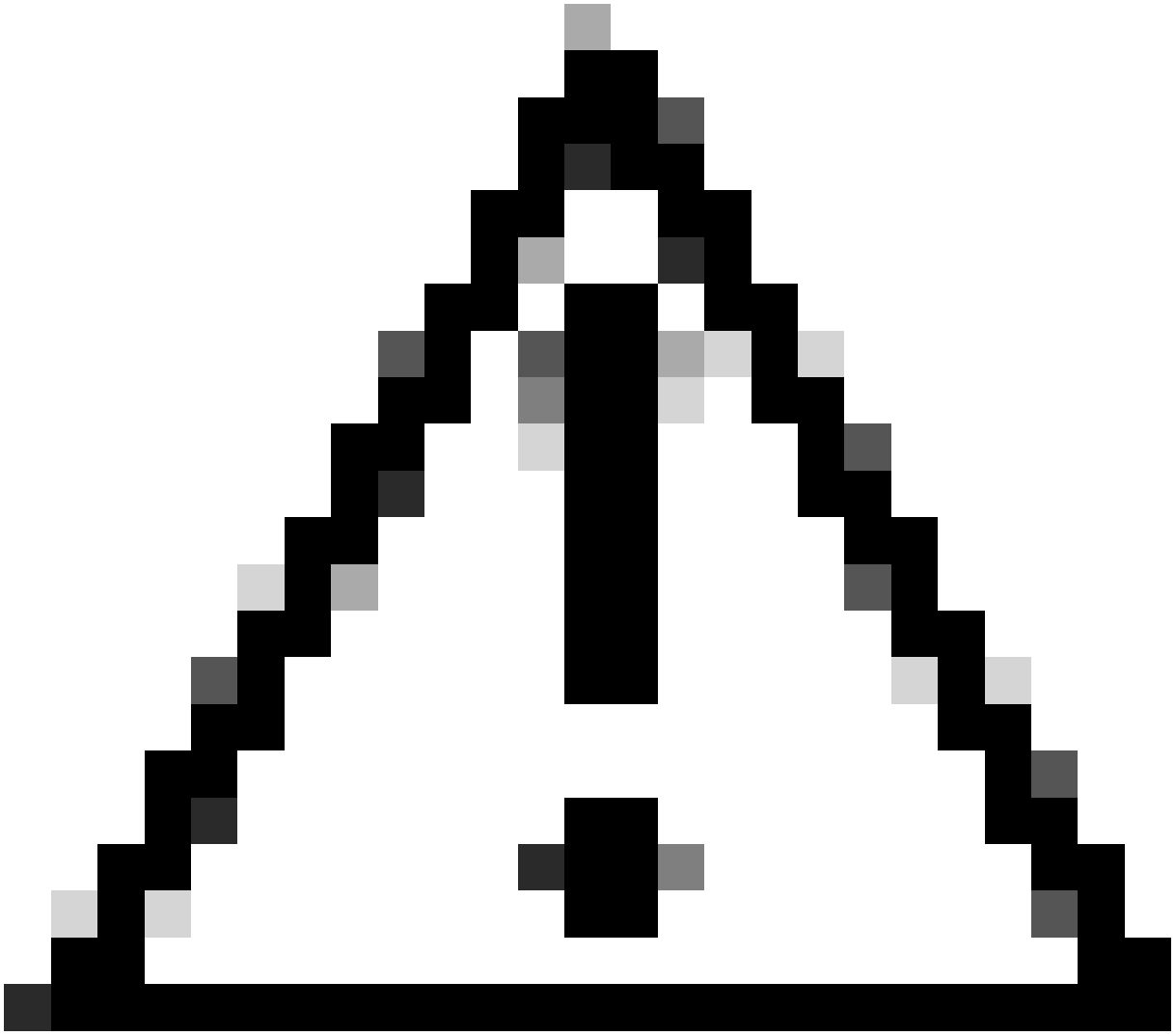
透過CLI：

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
```

透過GUI：導航至DHCP部分下的Configuration > Tags & Profile > Policy > Policy_name > Advanced. 啟用ipv4 DHCP required。



WLC上的策略配置檔案設定



注意：對於外部錨點設定，跨兩個WLC對齊DHCP設定非常重要。如果已啟用所需的IPV4 DHCP，則需要在外部WLC和錨點WLC上啟用它。兩者之間的策略配置檔案中的DHCP相關配置不一致可能導致客戶端在其移動角色時遇到問題。

問題2：由於IP竊取問題，客戶端被刪除或排除。在網路環境中，IP竊取是指多個無線客戶端嘗試使用同一IP地址的情況。原因有很多，如下所示：

1. 未授權的靜態IP分配：當使用者在其裝置上設定的靜態IP地址與網路上已分配或指定給使用者的IP地址相符時，可能會導致IP衝突。當兩台裝置嘗試使用相同的IP地址操作時，會出現這種情況，這可能會中斷相關裝置之一或兩台裝置的網路連線。要避免此類問題，必須確保為網路中的每個客戶端配置唯一的IP地址。

2. 惡意DHCP伺服器：網路上存在未經授權或惡意DHCP伺服器可能會導致IP地址分配與已建立的IP編址計畫發生衝突。此類衝突可能會導致多個裝置發生IP地址衝突或獲得不正確的網路設定。要解決此問題，應努力從網路中辨識並消除非法DHCP伺服器，以防止同一子網內出現進一步的IP衝突。

3. 9800 WLC中客戶端的過時條目：有時，控制器可能會保留客戶端嘗試獲取的IP地址的過時/過時條目。在這些情況下，必須手動從9800 WLC中刪除這些過時條目。以下是操作方法：

- 對排除清單中的mac地址運行放射性跟蹤，並用放射性跟蹤中的合法mac過濾該地址。
- 您將能夠看到錯誤日誌： %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON：客戶端MAC：具有IP：10.37.57.24的Affected_Client_MAC已增加到排除清單中，合法客戶端MAC： Legit_Client_MAC， IP： 10.37.57.24，原因：IP地址盜竊
- 然後執行下列指令：

show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(如果存在任何陳舊條目，您將可以看到一個合法客戶端Mac地址有多個IP：一個是原始IP，另一個是過時/陳舊的IP]。

解決方法：使用 clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. 在使用相同子網路的本機DHCP伺服器進行Flex部署時：在FlexConnect組態中，不同遠端位置通常使用從相同子網路指定IP位址的本機DHCP伺服器。這種情況可能導致位於不同站點的無線客戶端接收到相同的IP地址。此網路架構中的控制器被程式設計為檢測多個客戶端連線何時使用相同的IP地址，從而將其解釋為可能的IP盜竊。因此，這些客戶端通常被置於阻止清單中，以防止IP地址衝突。

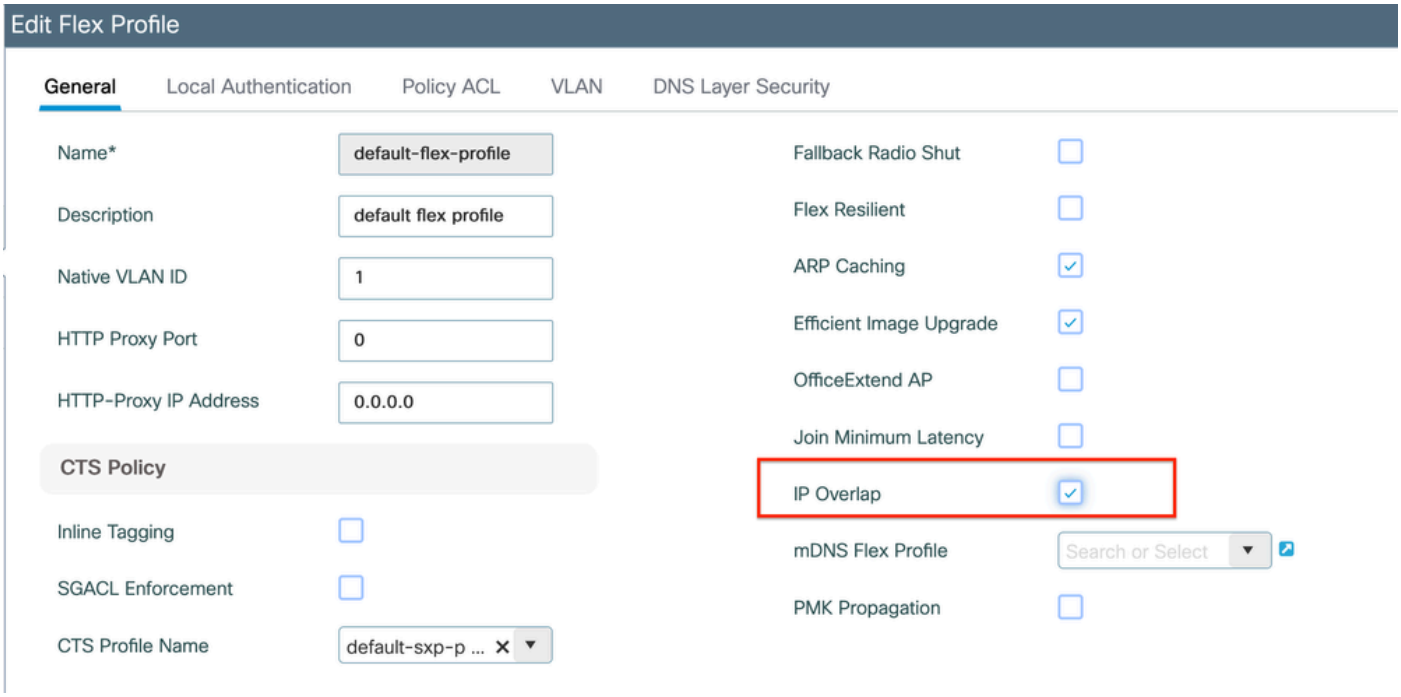
解決方案：在FlexConnect配置檔案中啟用IP重疊功能。「Flex Deployment中的重疊客戶端IP地址」功能允許在多個FlexConnect站點中使用相同的IP地址，同時維護FlexConnect部署中支援的所有特性和功能。

依預設，此功能為停用。您可以透過以下程式啟用它：

透過CLI：

```
configure terminal
 wireless profile flex $Flex_Profile_name
 ip overlap
```

透過GUI：選擇Configuration > Tags & Profiles > Flex. 點選現有Flex配置檔案/增加到新Flex配置檔案，並在General頁籤下啟用IP Overlap。



WLC上的Flex配置檔案設定

問題3.無線客戶端無法從預期的VLAN接收IP地址。在使用VLAN 1或分配給客戶端的VLAN與FlexConnect部署中用於AP管理的VLAN相同時，經常會發生此問題。此問題的根本原因通常是不正確的VLAN分配。為了提供指導，以下是在9800系列上設定VLAN ID時應考慮的幾個案例：

1. 採用啟用AAA覆蓋功能的AAA伺服器時，確保從AAA伺服器傳送適當的VLAN ID至關重要。如果提供了VLAN名稱，請確認它與9800 WLC上配置的VLAN名稱匹配。

2. 當為無線客戶端流量配置VLAN 1時，行為可能會因存取點(AP)的模式而異：

對於本地模式/集中交換中的AP：

- 指定VLAN-name =預設值，將客戶端分配給VLAN 1
- 使用VLAN-ID 1可將客戶端分配給無線管理VLAN

對於Flex模式/本地交換中的AP：

- 指定VLAN-name =預設值，將客戶端分配給VLAN 1
- 使用VLAN-ID 1可將客戶端分配給FlexConnect本地VLAN

以下是在實驗室中試驗過的一些案例的範例，及其結果：

1. 預設情況下，如果使用者未在策略配置檔案下配置任何內容，則WLC會分配VLAN-ID 1，以便客戶端在本地模式下使用無線管理VLAN，並為FlexConnect使用AP本地VLAN。

2. 如果flex-profile下的本地VLAN配置了不同於交換機上配置的本地VLAN ID，您會看到問題，即使策略配置檔案配置了「預設」VLAN名稱，客戶端也會從管理VLAN（本地VLAN）獲取IP。

3. 如果flex-profile下的Native-VLAN配置的VLAN-ID與交換機上配置的本地VLAN相同，則只有客戶端才能從策略配置檔案下配置了預設配置的VLAN 1獲取IP。

4. 如果選擇VLAN名稱而非VLAN ID，請確保Flex配置檔案中的VLAN名稱相同。

相關資訊

- 9800上的內部DHCP伺服器
- 外部DHCP伺服器正在使用
- Windows DHCP伺服器中的DHCP選項82子選項5
- Flex AP中的NAT-PAT
- VLAN 1用於無線客戶端
- 思科技術支援與下載

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）。