Cisco 9800 WLCでのDHCPクライアント接続問題のトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco 9800ワイヤレスLANコントローラ(WLC)に接続した際にワイヤレスクライアントで発生する、さまざまなDynamic Host Configuration Protocol(DHCP)関連の問題とそのトラブルシューティング方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco WLC 9800の基礎知識
- DHCPフローの基礎知識

- ローカルおよびフレックス接続モードのAPに関する基礎知識

ワイヤレスクライアントでのDHCPトラフィックのフローについて

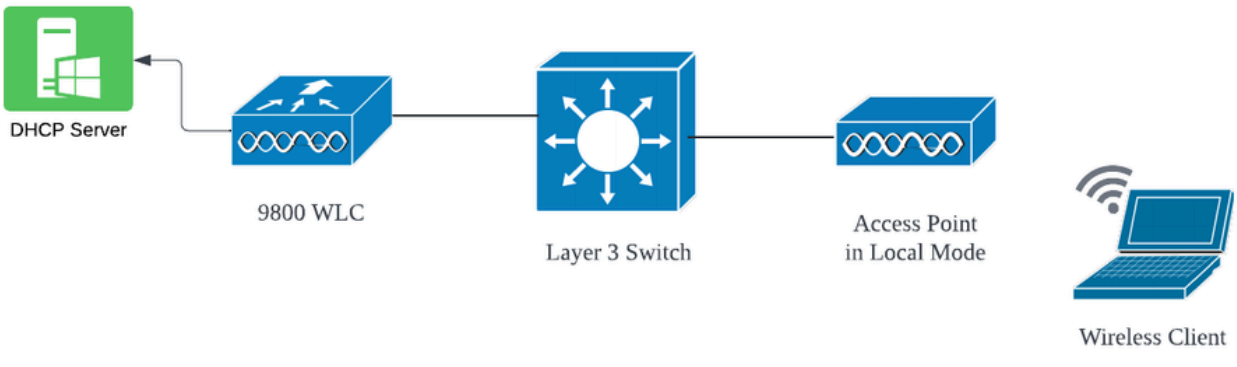
ワイヤレスクライアントは、接続すると、関連付けられたAPにDHCPサーバを検出するためにブロードキャストDHCPディスカバリフレームを送信することによって、通常のDHCP交換を行います。APの動作モードに応じて、CAPWAPトンネル経由でWLCに要求を転送するか、ネクストホップに要求を直接渡します。DHCPサーバがローカルのレイヤ2ドメイン内で使用可能な場合は応答し、接続の成功を促進します。ローカルサブネットのDHCPサーバがない場合は、DHCPディスカバリを適切なサーバにルーティングするようにルータ（クライアントのSVIで設定）を設定する必要があります。これは通常、特定のブロードキャストUDPトラフィック（DHCP要求など）をあらかじめ決められたIPアドレスに転送するようにルータに指示するIPヘルパーアドレスを設定することによって行われます。

クライアントDHCPトラフィックの動作は、アクセスポイント(AP)の動作モードに完全に依存します。これらの各シナリオを個別に見てみましょう。

シナリオ 1.アクセスポイント(AP)がローカルモードで動作している

APがローカルモードで設定されると、クライアントのDHCPトラフィックは中央でスイッチングされます。つまり、クライアントからのDHCP要求はAPからWLCへのCAPWAPトンネルを介して送信され、そこでAPは適切に処理されて転送されます。この場合、2つの選択肢があります。内部DHCPサーバを使用するか、外部DHCPサーバを選択します。

トポロジ（ローカルモードAP）



ケース スタディ 1WLCを内部DHCPサーバとして設定する場合

コントローラは、Cisco IOS XEソフトウェアの統合機能を通じて内部DHCPサーバを提供できます。ただし、外部DHCPサーバを使用することがベストプラクティスと考えられています。
WLCを内部DHCPサーバとして設定する前に、次の前提条件を満たす必要があります。

- クライアントVLANのスイッチ仮想インターフェイス(SVI)を設定し、DHCPサーバのIPアドレスを割り当ててください。
- 内部DHCPサーバのIPアドレスは、サーバ側のインターフェイスに設定する必要があります。このインターフェイスは、ループバックインターフェイス、SVI、またはレイヤ3物理インターフェイスになります。
- ループバックインターフェイスは、実際のネットワークセグメントに接続する物理インターフェイスとは異なり、ハードウェアに関連付けられず、デバイスの物理ポートに対応しないため、設定に推奨されます。ループバックインターフェイスの主な目的は、ハードウェア障害や物理的な切断の影響を受けない、安定した常時稼働インターフェイスを提供することです。

動作設定：クライアントが正常にIPアドレスを受信した内部DHCPサーバの設定例を次に示します。次に、操作ログと関連する設定の詳細を示します。

WLCをVLAN 10のDHCPサーバとして設定し、DHCPスコープの範囲を10.106.10.11/24 ~ 10.106.10.50/24にします。

```
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
```

WLCに設定されたループバックインターフェイス：

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

SVI [L3インターフェイス]として設定され、ヘルパーアドレスがWLCのループバックインターフェイスとして設定されたクライアントVLAN:

<#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
```

または、SVIでヘルパーアドレスを設定する代わりに、ポリシープロファイル内でDHCPサーバのIPアドレスを設定することもできます。ただし、一般的にはベストプラクティスのためにVLAN単位で設定することを推奨します。

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

WLCの放射性トレース：

```
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での組み込みパケットキャプチャ：

```
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での組み込みパケットキャプチャ

APクライアントのデバッグ

```
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>
```

クライアント側パケットキャプチャ：

```
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
```

クライアントエンドパケットキャプチャ

提供された操作ログから、WLCがワイヤレスクライアントからDHCP Discoverメッセージを受信し、クライアントのVLANがヘルパーアドレス (この例では内部ループバックインターフェイス) にメッセージをリレーしていることがわかります。その後、内部サーバがDHCPオファーを発行し、続いてクライアントがDHCP要求を送信します。この要求は、サーバによってDHCP ACKで確認応答されます。

ワイヤレスクライアントIPの確認：

WLC上：

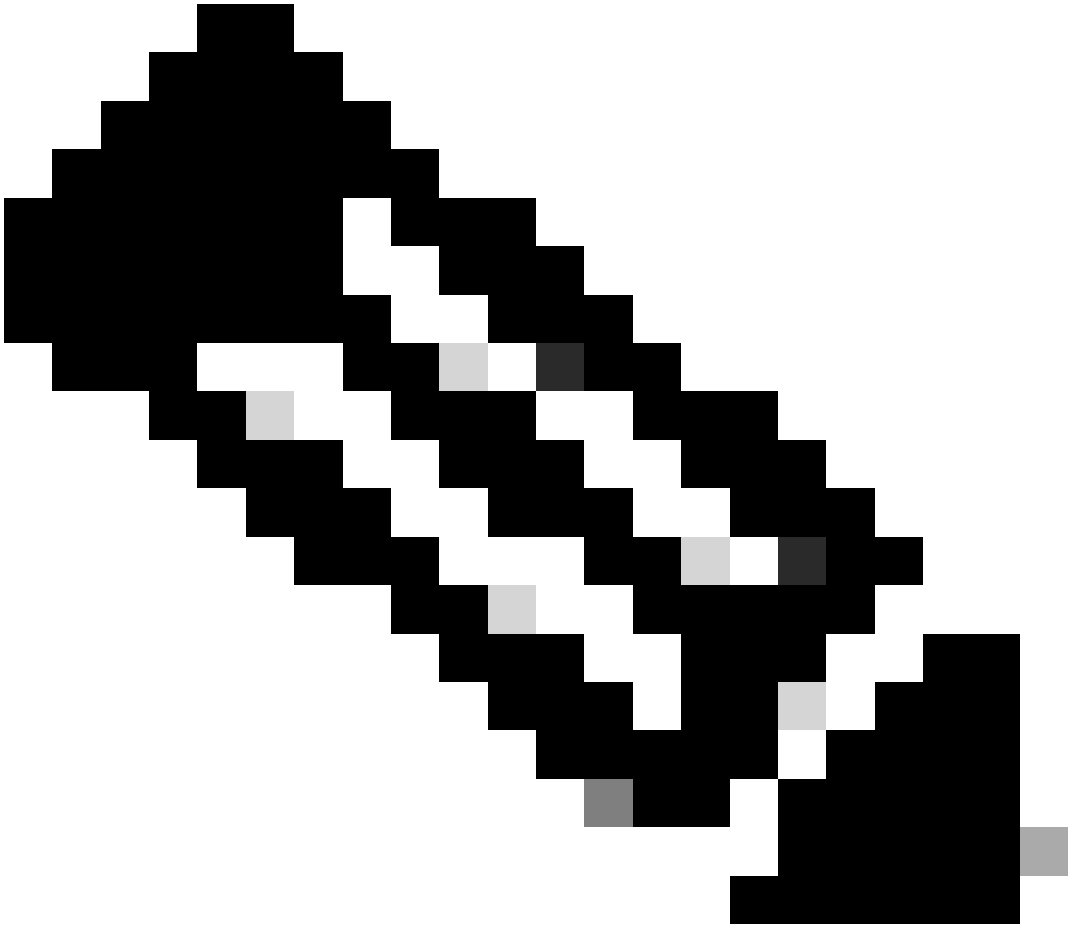
```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type          State
10.106.10.12     aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active     L
```

ワイヤレスクライアント：

```
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
```

クライアントエンドでのIP検証



注：
1. VRFは内部DHCPサーバではサポートされません。
2. DHCPv6は、内部DHCPサーバではサポートされていません。

---

3. C9800では、SVIによって複数のヘルパーアドレスの設定が可能ですが、最初の2つだけが使用されます。
4. これはテスト済みであるため、ボックスの最大クライアントスケールの20 %まで、すべてのプラットフォームでサポートされています。たとえば、64,000台のクライアントをサポートする9800-80の場合、サポートされる最大DHCPバインディングは約14,000です。

ケース スタディ 2外部DHCPサーバを使用する場合

外部DHCPサーバとは、WLC自体には統合されていないが、ネットワークインフラストラクチャ内の別のネットワークデバイス[ファイアウォール、ルータ]または別のエンティティ上に設定されているDHCPサーバを指します。このサーバは、ネットワーク上のクライアントに対するIPアドレスやその他のネットワーク設定パラメータの動的な配布を管理する専用サーバです。

外部DHCPサーバを使用する場合、WLCの機能はトラフィックの受信とリレーだけです。WLCからのDHCPトラフィックのルーティング方法は、ブロードキャストかユニキャストかに関係なく、設定によって異なります。これらの各方法を個別に検討してみましょう。

レイヤ2ドメインを介したDHCPトラフィックのブロードキャスト

この設定では、ファイアウォール、アップリンク、コアスイッチなどの別のネットワークデバイスがリレーエージェントとして機能します。クライアントがDHCPディスカバリ要求をブロードキャストする場合、WLCの唯一のジョブは、このブロードキャストをレイヤ2インターフェイス経由で転送することです。これが正しく機能するには、クライアントVLANのレイヤ2インターフェイスが正しく設定され、WLCのデータポートとアップリンクデバイスを介して許可されていることを確認する必要があります。

このインスタンスのクライアントVLAN 20に対してWLC側で必要な設定は、次のとおりです。

WLCでレイヤ2 VLANを設定した場合：

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

クライアントVLANのトラフィックを許可するようにWLCのデータポートを設定しました。

```
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の放射性トレース：

```
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 Client
```

9800 WLCで取得された組み込みパケットキャプチャ：

```
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での組み込みパケットキャプチャ

APクライアントのデバッグ

```
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>
```

クライアント側キャプチャ：

```
  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
```

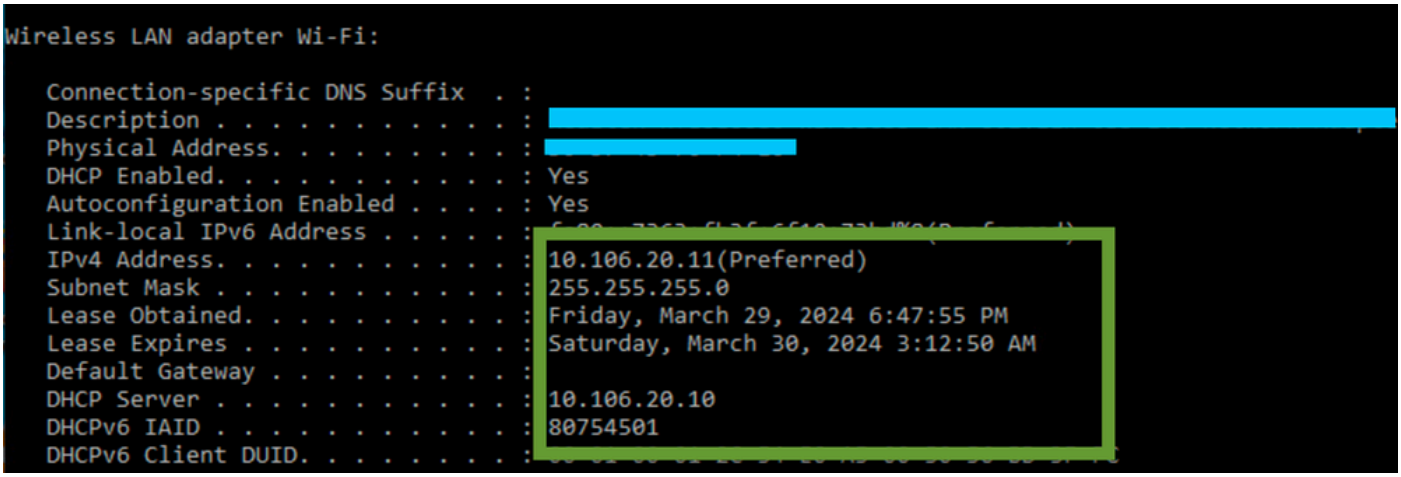
クライアントエンドパケットキャプチャ

提供された操作ログで、WLCがワイヤレスクライアントからのDHCP Discoverブロードキャストをインターセプトし、L2インターフェイスを介してネクストホップにブロードキャストしていることがわかります。WLCは、サーバからDHCPオファーを受信するとすぐに、このメッセージをクライアントに転送し、続いてDHCP要求とACKを送信します。

ワイヤレスクライアントIPの確認：

DHCPサーバのIPリースと対応するステータスを確認できます。

ワイヤレスクライアント：



クライアントエンドでのIP検証

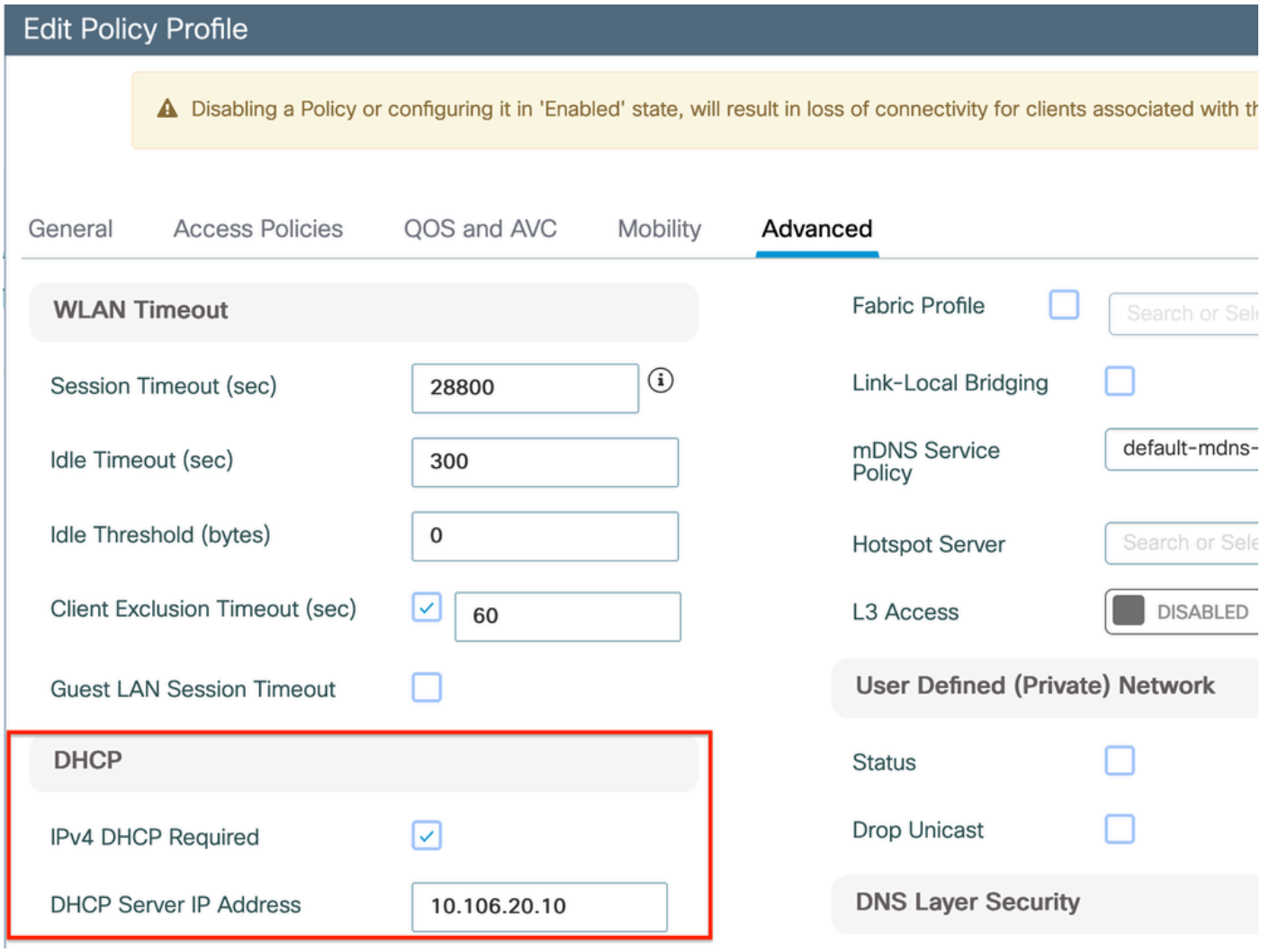
9800 WLCがリレーエージェントとして機能している

この設定では、WLCはワイヤレスクライアントから受信したDHCPパケットをユニキャストでDHCPサーバに直接転送します。これを有効にするには、クライアントのVLAN SVIがWLCで設定されていることを確認します。

9800 WLCでDHCPサーバIPを設定するには、次の2つの方法があります。

1. 拡張設定のポリシープロファイルでDHCPサーバのIPを設定します。

GUIを使用する場合：Configuration > Tags & Profile > Policy > Policy_name > Advanced. に移動します。DHCPセクションで、次に示すようにDHCPサーバのIPを設定できます。



WLCでのポリシープロファイルの設定

CLIを使用する場合：

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

2. SVI設定内で、ヘルパーアドレスを指定する必要があります。ヘルパーアドレス設定で複数のDHCPサーバを設定することで、冗長性を実現できます。ポリシープロファイル内の各WLANにDHCPサーバアドレスを設定することは可能ですが、推奨されるアプローチは、インターフェイス単位で設定することです。これは、ヘルパーアドレスを対応するSVIに割り当てることによって実現できます。

リレー機能を使用する場合、DHCPトラフィックの送信元は、クライアントのスイッチ仮想インターフェイス(SVI)のIPアドレスになります。このトラフィックは、ルーティングテーブルによって決定された宛先（DHCPサーバのIPアドレス）に対応するインターフェイスを介してルーティングされます。

次に、リレーエージェントとして動作する9800の動作設定の例を示します。

ヘルパーアドレスを使用してWLC上のクライアントVLAN用にレイヤ3インターフェイスを設定した場合：

```
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
```

クライアントVLANのトラフィックを許可するようにWLCのデータポートを設定しました。

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

WLCからのRAトレース：

```
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 Client
```

WLCでの組み込みパケットキャプチャ：

No.	Time	Source	Destination	Protocol	Lengtl	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での組み込みパケットキャプチャ

WLC上の放射性トレース(RA)とEmbedded Packet Capture(EPC)の両方で、リレーエージェントとして機能するWLCが、クライアン

トからDHCPサーバにDHCPパケットを直接ユニキャストしていることがわかります。

APクライアントのデバッグ

```
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>
```

クライアント側キャプチャ：

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

クライアントエンドパケットキャプチャ

ワイヤレスクライアントIPの確認：

DHCPサーバのIPリースと対応するステータスを確認できます。

ワイヤレスクライアント：

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . :
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .
   IPv4 Address. . . . . . . . . . . 10.106.20.12(Preferred)
   Subnet Mask . . . . . . . . . . . 255.255.255.0
   Lease Obtained. . . . . . . . . . Friday, March 29, 2024 9:53:53 PM
   Lease Expires . . . . . . . . . . Saturday, March 30, 2024 5:53:53 AM
   Default Gateway . . . . . . . . .
   DHCP Server . . . . . . . . . . . 10.106.20.10
   DHCPv6 IAID . . . . . . . . . . . 80754501
   DHCPv6 Client DUID. . . . . . . .
   DNS Servers . . . . . . . . . . . : 8.8.8.8
```

クライアントエンドでのIP検証

9800 WLCのサブオプション5/150でのDHCPオプション80

特定のシナリオでは、ネットワークが複雑になる可能性を防ぐために、ルーティングテーブルに依存するのではなく、DHCPトラフィックの送信元インターフェイスを明示的に定義する場合があります。これは、パス上の次のネットワークデバイス（レイヤ3スイッチやファイアウォールなど）がリバースパス転送(RPF)チェックを使用する場合に特に重要です。たとえば、ワイヤレス管

理インターフェイスがVLAN 50に設定されている一方で、クライアントSVIがVLAN 20にあり、クライアントトラフィックのDHCPリレーとして使用されている状況を考えます。デフォルトルートは、ワイヤレス管理VLAN/サブネットのゲートウェイに向けられています。

9800 WLCのバージョン17.03.03から、DHCPトラフィックの送信元インターフェイスとして、クライアントVLANまたはWireless Management Interface(WMI)などの別のVLANを選択できます。これにより、DHCPサーバへの接続が保証されます。

設定の抜粋を次に示します。

```
!
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
```

このシナリオでは、DHCPサーバ10.100.17.14へのトラフィックの発信元がVLAN 50(10.100.16.10)になります。これは、パケットの出力インターフェイスがIPルーティングテーブルでのルックアップに基づいて選択され、通常はデフォルトルートが設定されているため、ワイヤレス管理インターフェイス(WMI)VLAN経由で出力されるためです。
ただし、アップリンクスイッチでReverse Path Forwarding（RPF；リバースパス転送）チェックが実装されている場合は、VLAN 50から到達した、送信元IPアドレスが異なるサブネット[VLAN 20]に属するパケットが廃棄される場合があります。

これを防ぐには、IP DHCP relay source-interfaceコマンドを使用して、DHCPパケットに正確な送信元インターフェイスを設定する必要があります。この特定のケースでは、DHCPパケットをVLAN 50のWMIインターフェイスから発信します。

```
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
```

ip dhcp relay source-interfaceコマンドを使用すると、DHCPパケットの送信元インターフェイスとGIADDRの両方が、DHCPリレーコマンドで指定されたインターフェイス（この場合はVLAN50）に設定されます。これは、DHCPアドレスを割り当てるクライアントVLANではないため、問題になります。

DHCPサーバは適切なクライアントプールからIPを割り当てる方法をどのように認識しますか。

したがって、これに対する答えは、ip dhcp relay source-interface コマンドが使用されたときに、C9800が自動的にクライアントサブ

ネット情報をオプション82の独自のサブオプション150に追加することです。これはリンク選択と呼ばれ、キャプチャから確認できます。

```
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
```

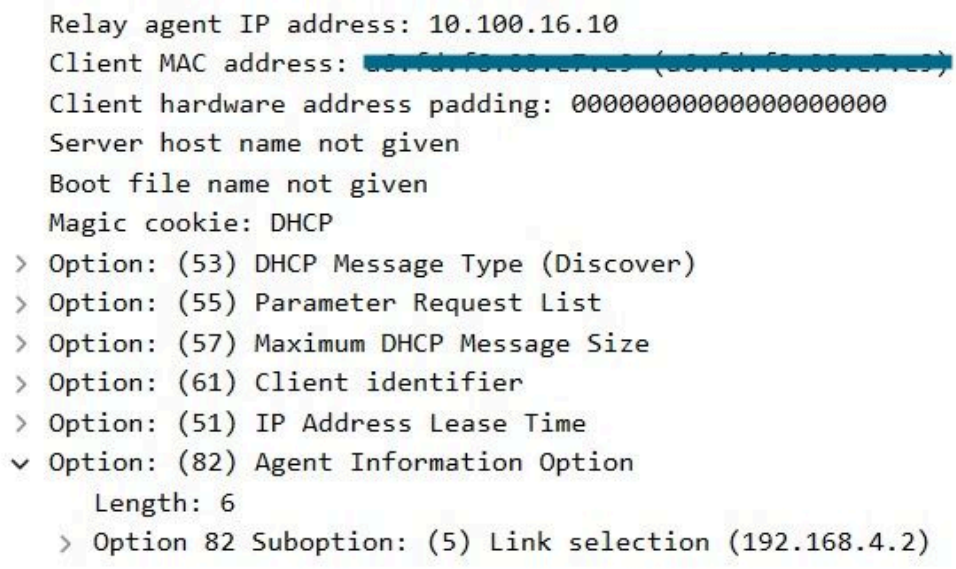
*WLC*パケットキャプチャのオプション182サブオプション150

デフォルトでは、サブオプション150（シスコ独自）が追加されます。使用するDHCPサーバがこの情報を解釈し、この情報に基づいて動作できることを確認します。C9800の設定を変更し、標準オプション82、サブオプション5を使用してリンク選択情報を送信することをお勧めします。これを行うには、次のグローバルコマンドを設定します。

```
<#root>

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

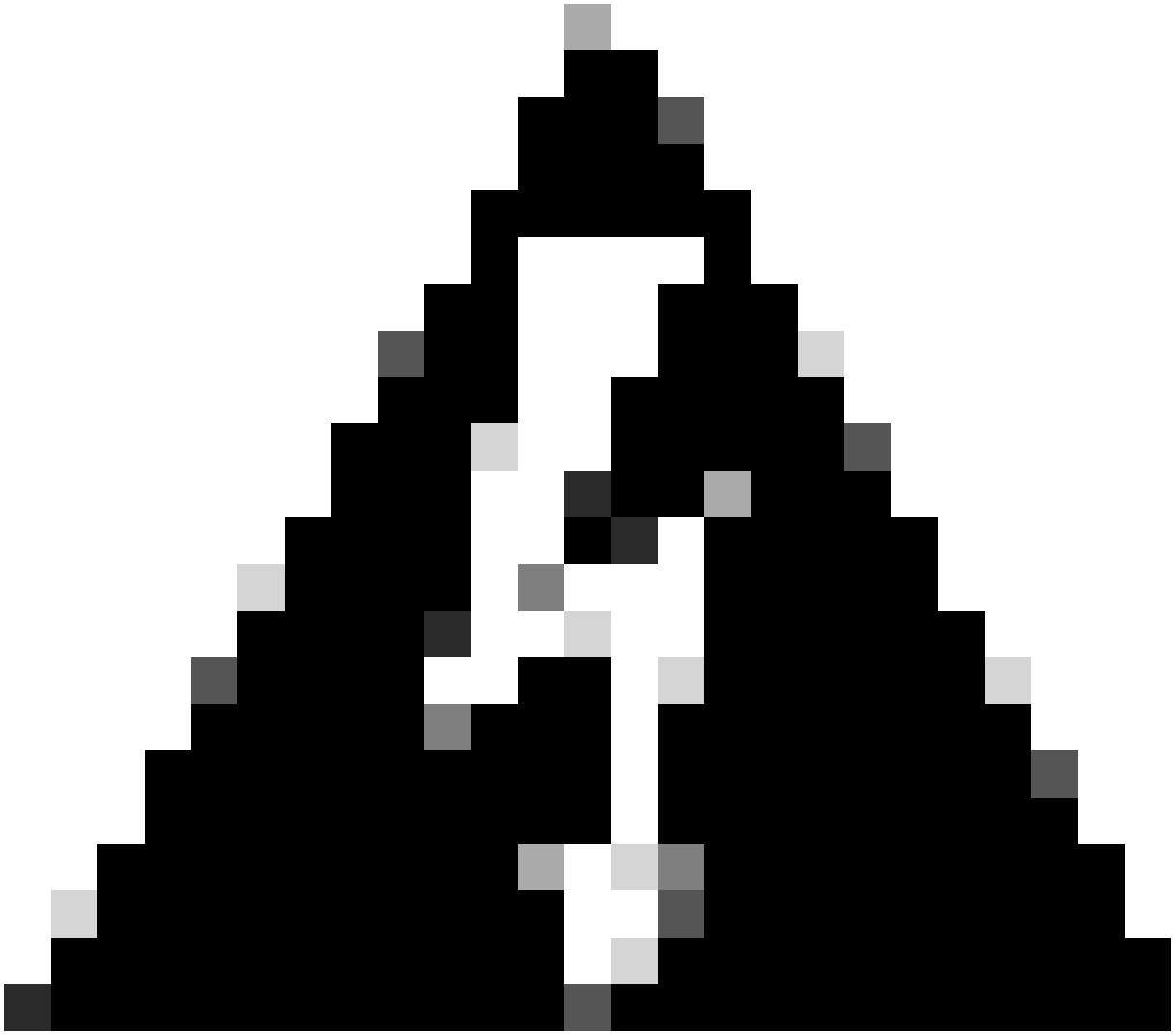
指定したコマンドが適用されると、システムはDHCPパケットでサブオプション150をサブオプション5に置き換えます。サブオプション5はネットワークデバイスで広く認識されているため、パケットが廃棄される可能性が低くなります。この変更の適用は、提供されるキャプチャでも明らかです。



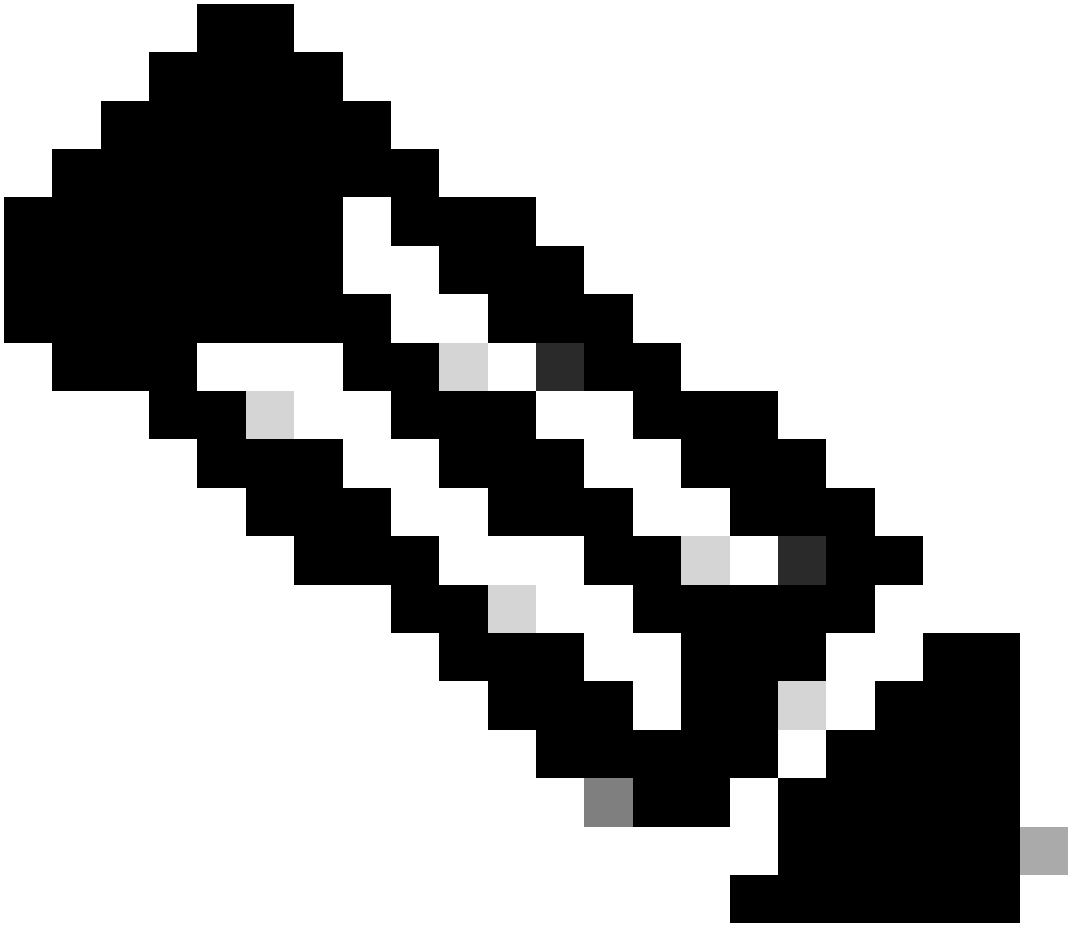
WLCパケットキャプチャのオプション182サブオプション5

サブオプション5を実装すると、DHCPトラフィックは他のネットワークデバイスによって確認応答されます。ただし、特にWindows DHCPサーバが使用中の場合は、NAK（否定応答）メッセージが引き続き表示されることがあります。これは、DHCPサーバが送信元IPアドレスを認可していないことが原因である可能性があります。その原因として、その送信元IPに対応する設定がないことが考えられます。

DHCPサーバでは何を行う必要がありますか。Windows DHCPサーバでは、リレーエージェントのIPを認可するためにダミーのスコープを作成する必要があります。



警告：すべてのリレーエージェントのIPアドレス(GIADDR)は、アクティブなDHCPスコープのIPアドレス範囲に含まれている必要があります。DHCPスコープのIPアドレス範囲外のGIADDRは不正なリレーと見なされ、Windows DHCPサーバはこれらのリレーエージェントからのDHCPクライアント要求を許可しません。リレーエージェントを許可するための特別なスコープを作成できます。GIADDRでスコープを作成し（GIADDRが連続したIPアドレスの場合は複数）、配布からGIADDRアドレスを除外し、スコープをアクティブにします。これにより、GIADDRアドレスの割り当てを防ぎながら、リレーエージェントを許可します。

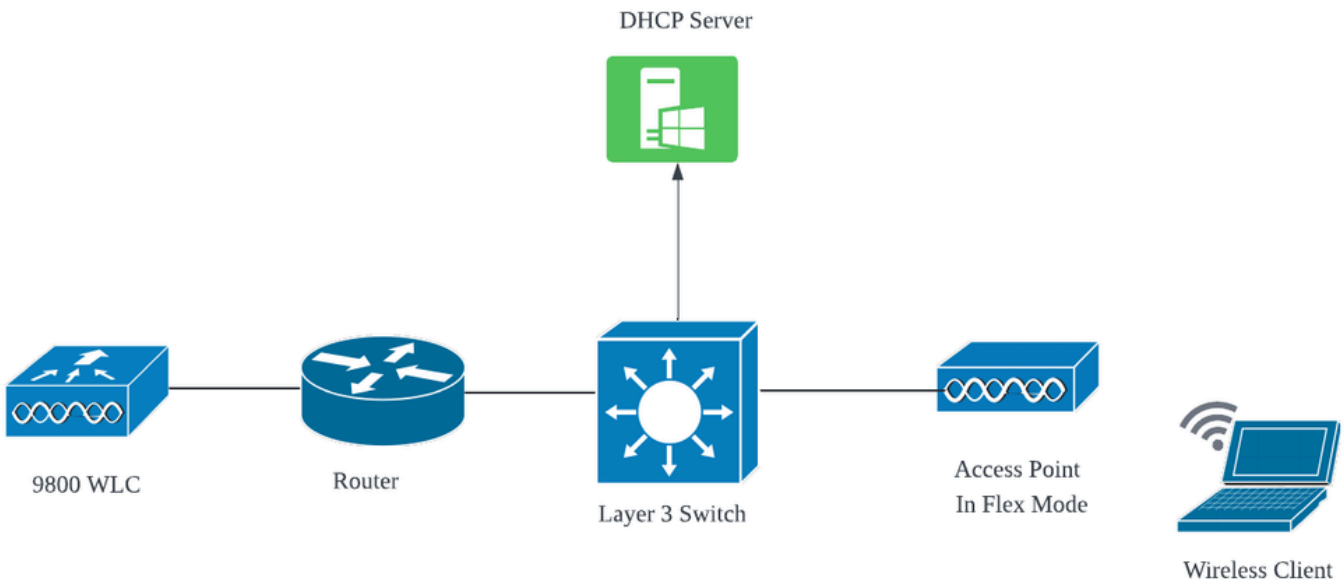


注：外部アンカー設定では、DHCPトラフィックはローカルとして設定されたAPモードで一元的に処理されます。最初に、DHCP要求が外部WLCに送信され、外部WLCはモビリティトンネル経由でアンカーWLCに転送します。設定された設定に従ってトラフィックを処理するのは、アンカーWLCです。したがって、DHCPに関連するすべての設定をアンカーWLCに実装する必要があります。

シナリオ 2.アクセスポイント(AP)がFlexモードで動作している

FlexConnect APは、ブランチオフィスやリモートオフィス向けに設計されており、中央のワイヤレスLANコントローラ(WLC)への接続が失われたときに、スタンドアロンモードで動作できます。FlexConnect APは、トラフィックをWLCにバックホールすることなく、クライアントとネットワークの間でトラフィックをローカルにスイッチングできます。これにより、遅延が減少し、WAN帯域幅が節約されます。フレックスモードAPでは、DHCPトラフィックは中央でスイッチングするか、ローカルでスイッチングすることができます。

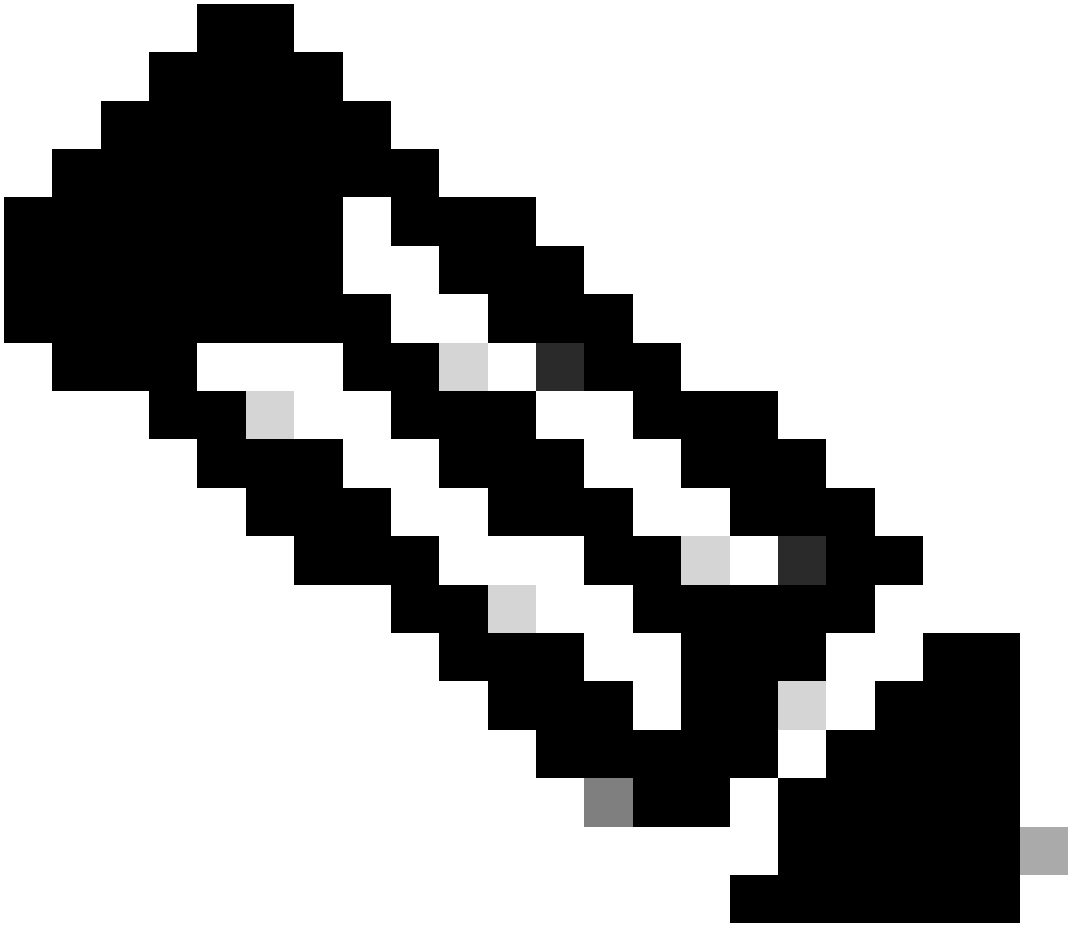
トポロジ（フレックスモードAP）



ネットワークトポロジ：フレックスモードAP

中央DHCPを使用するFlexConnectモードのAP

中央のDHCPサーバを使用する場合は、APモードに関係なく、設定、操作フロー、およびトラブルシューティングの手順は一貫しています。ただし、FlexConnectモードのAPの場合、ローカルサイトでクライアントSVIを設定していない限り、通常はローカルDHCPサーバを使用することをお勧めします。



注：リモートサイトでクライアントサブネットを使用できない場合は、FlexConnect NAT-PATを利用できます。FlexConnect NAT/PATは、APに接続されたクライアントから発信されたトラフィックのネットワークアドレス変換(NAT)を実行し、APの管理IPアドレスにマッピングします。たとえば、リモートブランチのFlexConnectモードで動作するAPがあり、接続されたクライアントがコントローラが存在する本社にあるDHCPサーバと通信する必要がある場合、ポリシープロファイルの中央DHCP設定と連動してFlexConnect NAT/PATをアクティブ化できます。

ローカルDHCPを使用するFlexConnectモードのAP

FlexConnect APがローカルDHCPを使用するように設定されている場合、APにアソシエートするクライアントデバイスは、同じローカルネットワーク内で使用可能なDHCPサーバからIPアドレス設定を受信します。このローカルDHCPサーバは、ルータ、専用DHCPサーバ、またはローカルサブネット内でDHCPサービスを提供するその他のネットワークデバイスです。ローカルDHCPでは、DHCPトラフィックはローカルネットワーク内でスイッチングされます。つまり、APはDHCP要求をクライアントからアクセススイッチなどの隣接ホップに直接リレーします。そこから、要求はネットワークの設定に従って処理されます。

前提条件：

1. FlexConnectガイドを参照して、ご使用の設定がガイドに記載されている手順とベストプラクティスに合致していることを確認してください。

2. クライアントVLANは、Flex Profileの下にリストされる必要があります。
3. APをトランクモードで設定し、AP管理VLANをネイティブVLANとして指定する必要があります。また、クライアントトラフィック用のVLANをトランクで許可する必要があります。

管理VLANを58、クライアントVLANを20に設定したAP接続スイッチポートの設定例を次に示します。

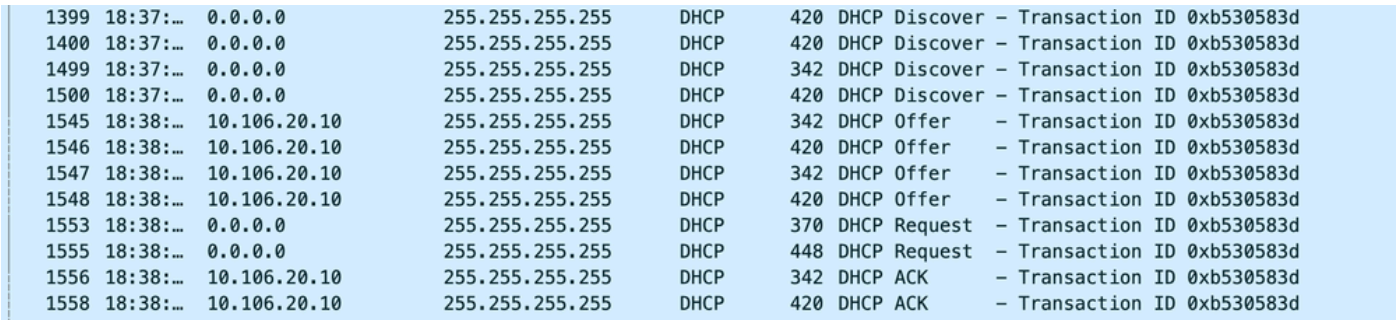
```
Switch#show run int gig1/0/2
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 20,58
switchport trunk encapsulation dot1q
switchport trunk native vlan 58
switchport mode trunk
end
!
```

作業セットアップ：APがFlexモードに設定されている場合に、ローカルDHCPサーバと運用ログを共有するための参考資料：

APクライアントのデバッグ

```
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アップリンクキャプチャ：



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アップリンクキャプチャ

クライアント側キャプチャ：

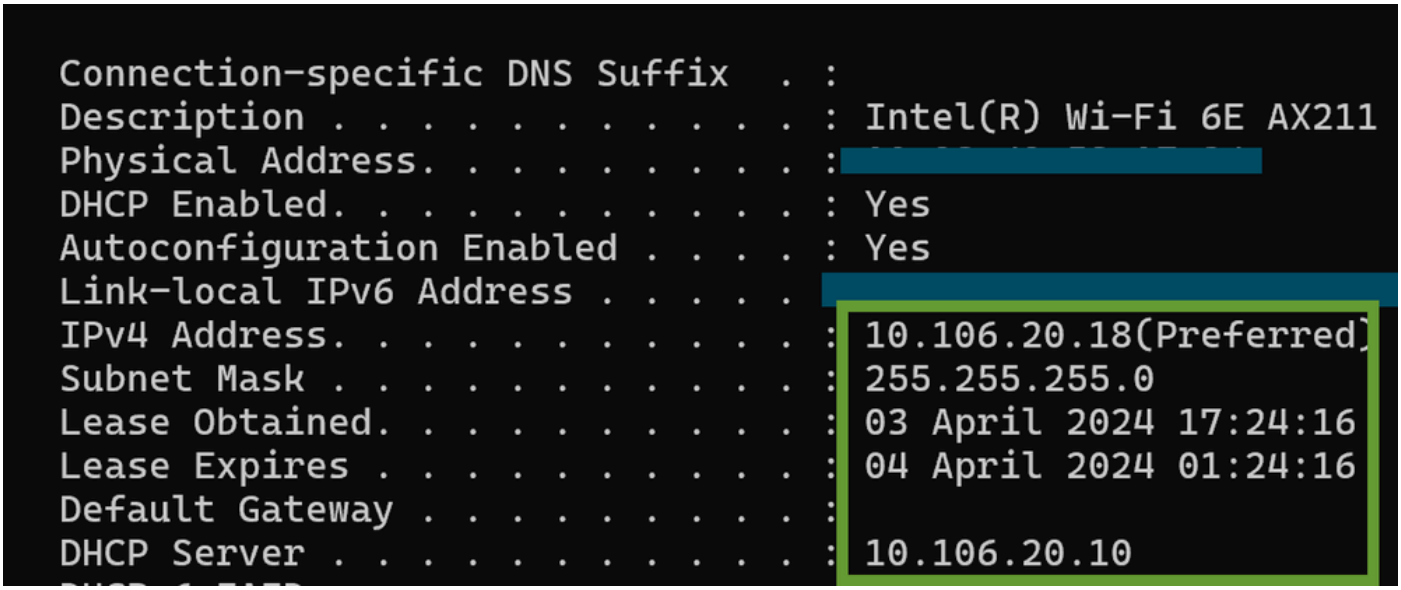
```
16540 111.905836    0.0.0.0          255.255.255.255    DHCP     343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18       DHCP     342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255    DHCP     385 DHCP Request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

クライアントエンドパケットキャプチャ

ワイヤレスクライアントIPの確認：

DHCPサーバのIPリースと対応するステータスを確認できます。

ワイヤレスクライアント：



クライアントエンドでのIP検証

DHCP問題のトラブルシューティング

DHCP問題のトラブルシューティングには、クライアントがワイヤレスネットワークに接続するときにDHCPサーバからIPアドレスを取得できない問題を特定して解決することが含まれます。DHCPの問題をトラブルシューティングする際の一般的な手順と考慮事項を次に示します。

1. クライアント設定の確認

- クライアントがIPアドレスを自動的に取得するように設定されていることを確認します。
- ネットワークアダプタが有効で正常に機能していることを確認します。

2. DHCPサーバーの状態を確認する

- DHCPサーバが動作していて、クライアントのネットワークセグメントから到達可能であることを確認します。
- DHCPサーバのIPアドレス、サブネットマスク、およびデフォルトゲートウェイの設定を確認します。

3. スコープ構成の確認

- DHCPスコープを調べて、クライアントが使用できるIPアドレスの十分な範囲があることを確認します。
- スコープのリース期間とオプション（DNSサーバ、デフォルトゲートウェイなど）を確認します。
- 一部の環境（Active Directoryなど）では、ネットワーク内でDHCPサービスを提供する権限がDHCPサーバに与えられていることを確認します。

4. 9800 WLCの設定の確認

- ループバックインターフェイス、クライアントSVIの欠如、設定されたヘルパーアドレスの欠如など、設定ミスが原因で発生する問題は数多くあります。ログを収集する前に、設定が正しく実装されていることを確認することをお勧めします。
- 内部DHCPサーバを利用する場合：DHCPスコープの枯渇に関しては、特にCLIからDHCPを設定する場合は、リースタイマーが要件に従って設定されていることを確認することが重要です。デフォルトでは、9800 WLCのリースタイマーは無限に設定されています。
- 中央のDHCPサーバを使用する場合は、クライアントVLANトラフィックがWLCのアップリンクポートで許可されることを確認します。逆に、ローカルDHCPサーバを採用する場合は、関連するVLANがAPアップリンクポートで許可されていることを確認します。

5. ファイアウォールとセキュリティの設定

- ファイアウォールまたはセキュリティソフトウェアがDHCPトラフィック（DHCPサーバのポート67、DHCPクライアントのポート68）をブロックしていないことを確認します。

ログ収集

WLCからのログ

1. すべてのコマンドの時間参照を含めるために、term exec prompt timestampを有効にします。

2. show tech-support wireless !! を使用して、設定を確認します。

2. クライアントの数、クライアント状態の配布、および除外されたクライアントを確認できます。
show wireless summary !! APおよびクライアントの総数
show wireless exclusionlist !! クライアントが除外されていると見なされる場合
show wireless exclusionlist client mac-address MAC@ !! 除外する具体的なクライアントの詳細を取得し、その理由が任意のクライアントのIP盗難としてリストされているかどうかを確認します。

3. クライアントのIPアドレス割り当てを確認し、不正なアドレスや予期しないスタティックアドレスの学習、DHCPサーバからの応答がないためにダーティとマークされたVLAN、またはDHCP/ARPを処理しているSISFでのパケットドロップを探します。

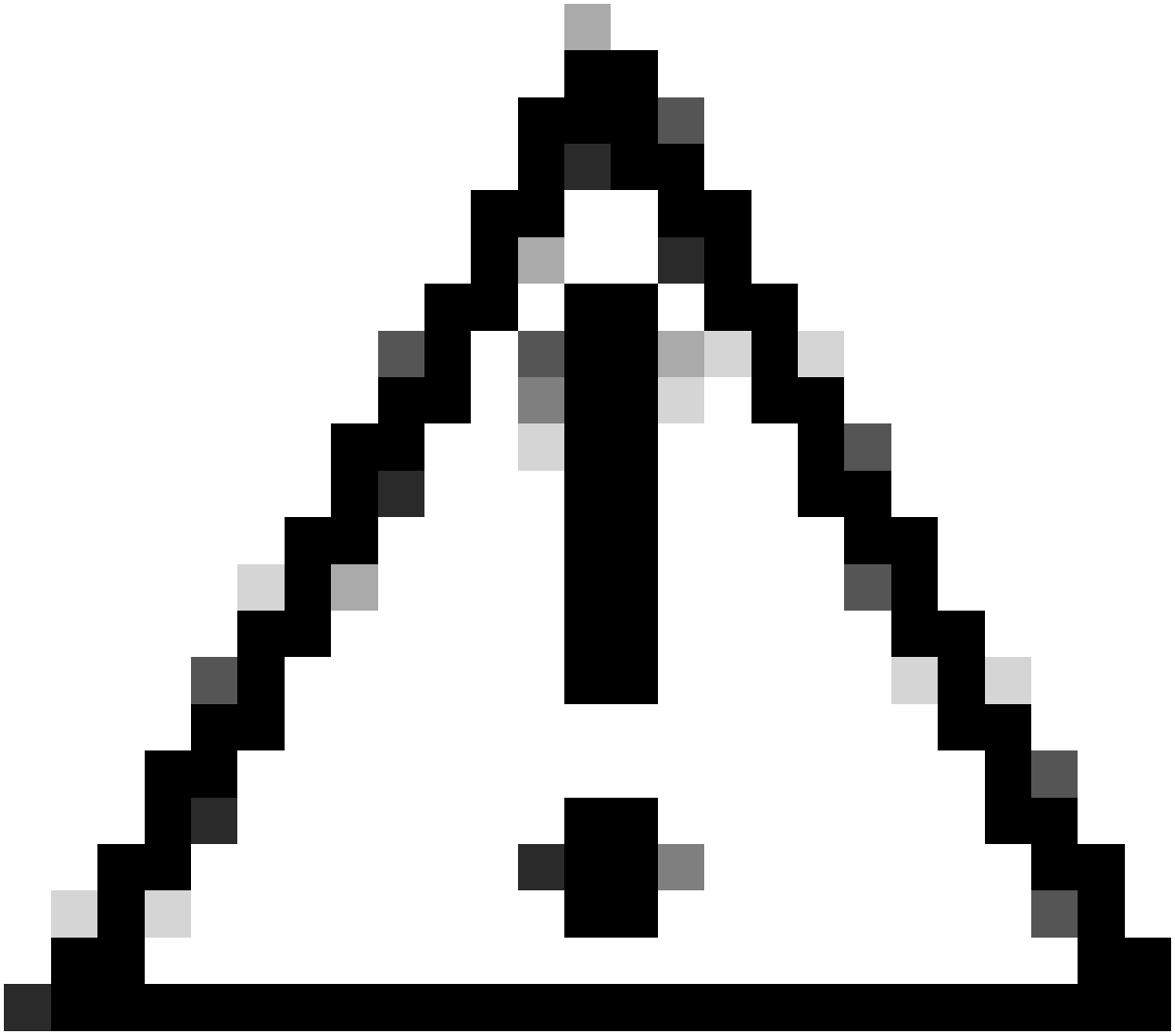
show wireless device-tracking database ip !! IPで確認し、アドレス学習がどのように行われたかを確認します。
show wireless device-tracking database mac !! Macを調べて、どのIPクライアントが割り当てられているのかを確認します。
show wireless vlan details !! 使用中のVLANグループの場合、DHCP障害によりVLANがダーティとしてマークされていないことを確認します。
show wireless device-tracking feature drop !!SISFでのドロップ

4. 具体的なクライアントMAC@に関するWLCからの特定の出力 show wireless device-tracking feature drop

クライアントがワイヤレスネットワークに接続しようとしているときに、クライアントのMACアドレスの放射性トレースを有効にします。

CLIを使用する場合：

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：条件付きデバッグを使用すると、デバッグレベルのロギングが有効になり、生成される ログの量が増加します。これを実行したままにすると、ログを表示できる時間を短縮できます。そのため、トラブルシューティングセッションの最後には常にデバッグを無効にすることを推奨します。

すべてのデバッグを無効にするには、次のコマンドを実行します。

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

GUI 経由:

ステップ 1：移動先 Troubleshooting > Radioactive Trace .
ステップ 2：Addをクリックし、トラブルシューティングを行うクライアントのMACアドレスを入力します。追跡するMacアドレスを複数追加できます。

ステップ 3：放射性トレースを開始する準備ができたら、[開始]をクリックします。いったん開始すると、追跡されるMACアドレスに関連するコントロールプレーンの処理に関するデバッグロギングがディスクに書き込まれます。

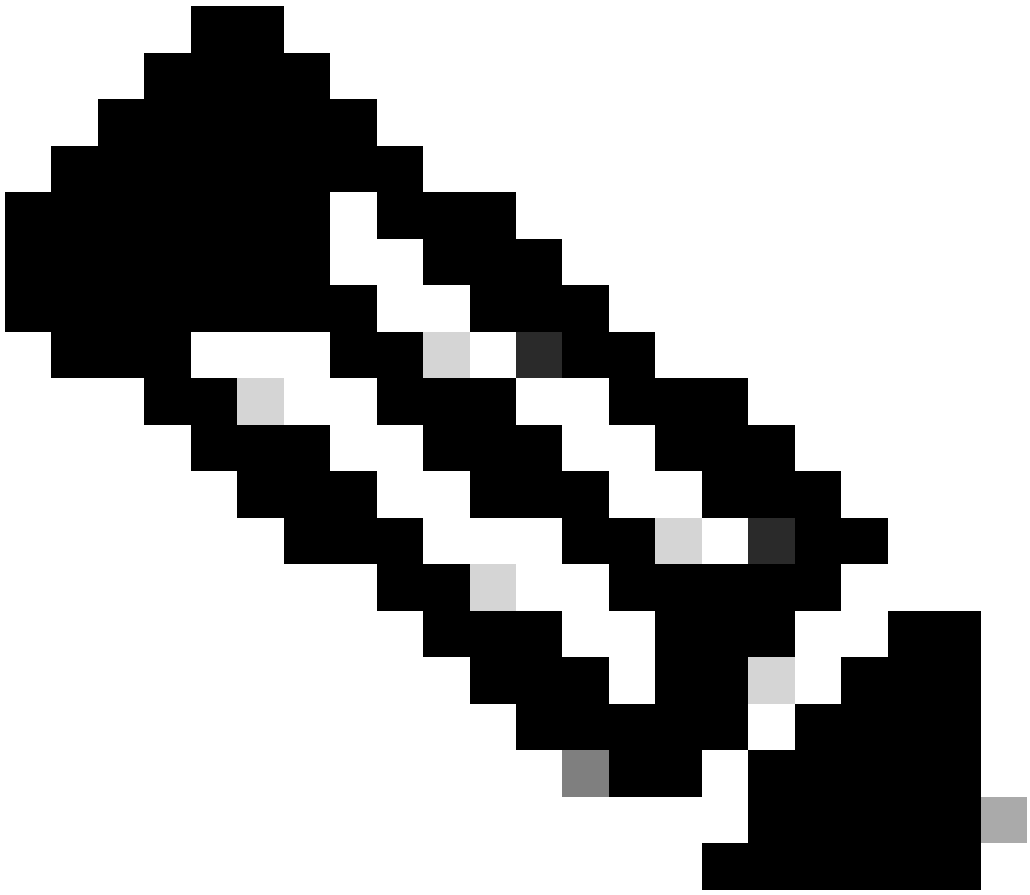
ステップ 4：トラブルシューティングする問題を再現したら、Stopをクリックします。

ステップ 5：デバッグしたMACアドレスごとに、 Generate をクリックして、そのMACアドレスに関連するすべてのログを集計するログファイルを生成できます。

手順 6：照合済みログファイルの取得時間を選択し、[デバイスに適用]をクリックします。

手順 7：ファイル名の横にある小さいアイコンをクリックすると、ファイルをダウンロードできます。このファイルはコントローラのブートフラッシュドライブにあり、CLIを使用してコピーすることもできます。

!!クライアントのMACアドレスによって双方向にフィルタリングされた組み込みキャプチャ。クライアントの内部MACフィルタは17.1以降で使用可能。



注:9800のEPCは、9800 WLCで中央DHCPが有効になっている場合に役立ちます。

CLIを使用する場合：

```
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
```

GUI 経由:
ステップ 1：Troubleshooting > Packet Capture > +Addに移動します。

ステップ 2：パケットキャプチャの名前を定義します。最大8文字まで入力できます。

ステップ 3：フィルタを定義します（存在する場合）。

ステップ 4：トラフィックがシステムCPUにパントされ、データプレーンに再び注入されるのを確認する場合は、Monitor Control Trafficのボックスにチェックマークを付けます。

ステップ 5：バッファサイズを定義します。最大100 MBまで使用できます。

手順 6：必要に応じて、1 ~ 1000000秒の範囲を許容する期間ごと、または1 ~ 100000パケットの範囲を許容するパケット数ごとに制限を定義します。

手順 7：左側の列のインターフェイスのリストからインターフェイスを選択し、矢印を選択して右側の列に移動します。

ステップ 8：保存してデバイスに適用

ステップ 9：キャプチャを開始するには、[開始]を選択します。

ステップ 10：キャプチャを定義された制限まで実行できます。キャプチャを手動で停止するには、[停止]を選択します。

ステップ 11停止すると、Exportボタンが使用可能になり、HTTPまたはTFTPサーバ、FTPサーバ、あるいはローカルシステムのハードディスクまたはフラッシュを介してローカルデスクトップにキャプチャファイル(.pcap)をダウンロードするオプションが表示されます。

AP側からのログ

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

```
!!Basic
debug client MAC@
```

DHCPサーバからのログ

外部DHCPサーバを使用する場合、DHCPトラフィックのフローを確認するには、サーバ側でデバッグログとパケットキャプチャを収集する必要があります。

その他のログ

9800 WLCでDHCP検出メッセージが中央のDHCP設定またはローカルのDHCP設定のAPデバッグログに表示される場合は、アップリンクからキャプチャデータを収集して、パケットがイーサネットポートでドロップされていないことを確認する必要があります。スイッチの機能に応じて、アップリンクスイッチで組み込みパケットキャプチャまたはSPAN（スイッチドポートアナライザ）キャプチャを実行できます。DHCPクライアントからDHCPサーバへの通信が中断されたポイントを判別するため、および逆方向の通信が中断されたポイントを判別するために、DHCPトラフィックフローを段階的にトレースすることをお勧めします。

既知の問題

問題 1.クライアントは、以前に保持していたVLANからIPアドレスを取得しようとしています。ワイヤレスクライアントが、異なるクライアントVLANに関連付けられた2つのSSID間で切り替わる場合があります。このような場合、クライアントは以前に接続したVLANからIPを要求し続ける可能性があります。このIPは現在のVLANのDHCPスコープ内にないため、DHCPサーバはNAK（否定応答）を発行し、その結果、クライアントはIPアドレスを取得できなくなります。

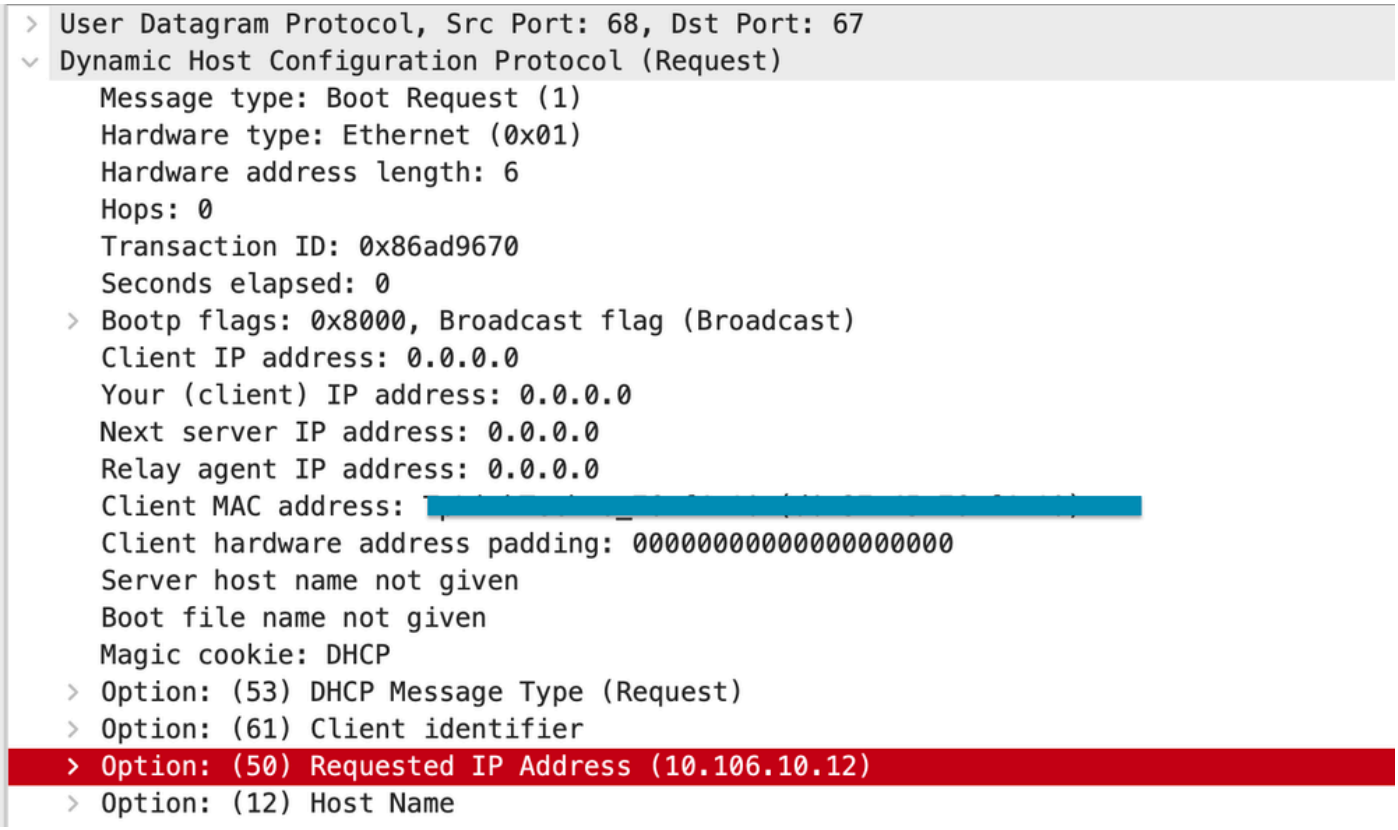
放射性トレースログでは、現在のSSIDのクライアントVLANがVLAN 20であるにもかかわらず、クライアントが以前に接続していたVLAN(VLAN 10)からIPを探し続けていることがわかります。

```
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での組み込みパケットキャプチャ：

```
166 16:10:…  0.0.0.0          255.255.255.255    DHCP    368 DHCP Request  - Transaction ID 0x86ad9670
167 16:10:…  0.0.0.0          255.255.255.255    DHCP    368 DHCP Request  - Transaction ID 0x86ad9670
168 16:10:…  10.106.20.10     255.255.255.255    DHCP    346 DHCP NAK      - Transaction ID 0x86ad9670
169 16:10:…  10.106.20.10     255.255.255.255    DHCP    346 DHCP NAK      - Transaction ID 0x86ad9670
```

WLCでの組み込みパケットキャプチャ



WLCでのDHCPオプション50のパケットキャプチャ

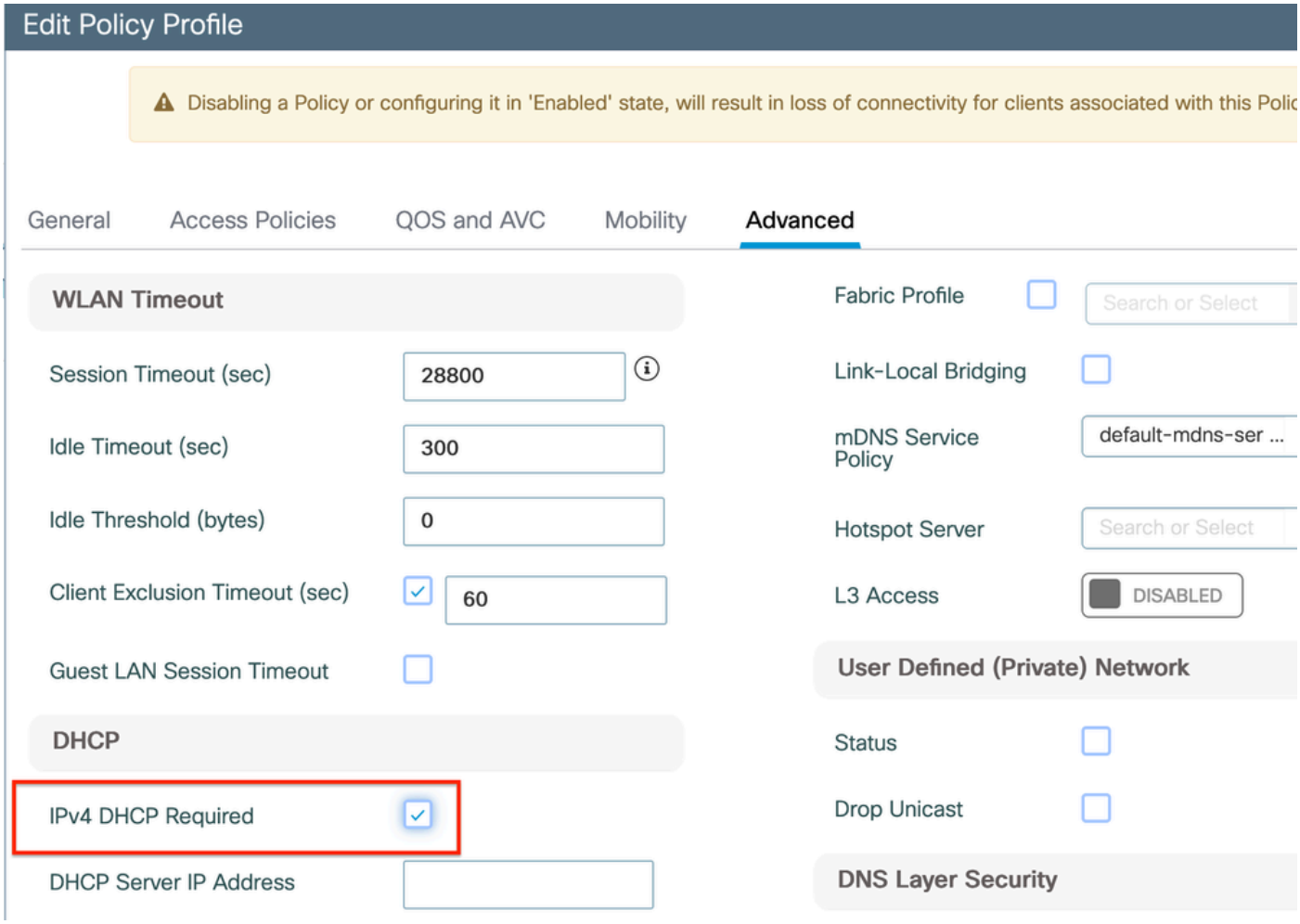
解決策：クライアントが完全なDHCPプロセスを完了するようにするには、ポリシー設定でIPv4 DHCP Requiredオプションを有効にします。クライアントがSSID間で切り替えを行っている場合は特に、この設定を有効にして、以前のSSIDに関連付けられたVLANからIPアドレスを要求する場合に、DHCPサーバがクライアントにNAKを送信できるようにします。そうしないと、クライアントは以前に保持していたIPアドレスを引き続き使用または要求し、通信が中断される可能性があります。ただし、この機能を有効にすると、スタティックIPアドレスを使用して設定されているワイヤレスクライアントに影響を与えることに注意してください。

目的のオプションを有効にするプロセスを次に示します。

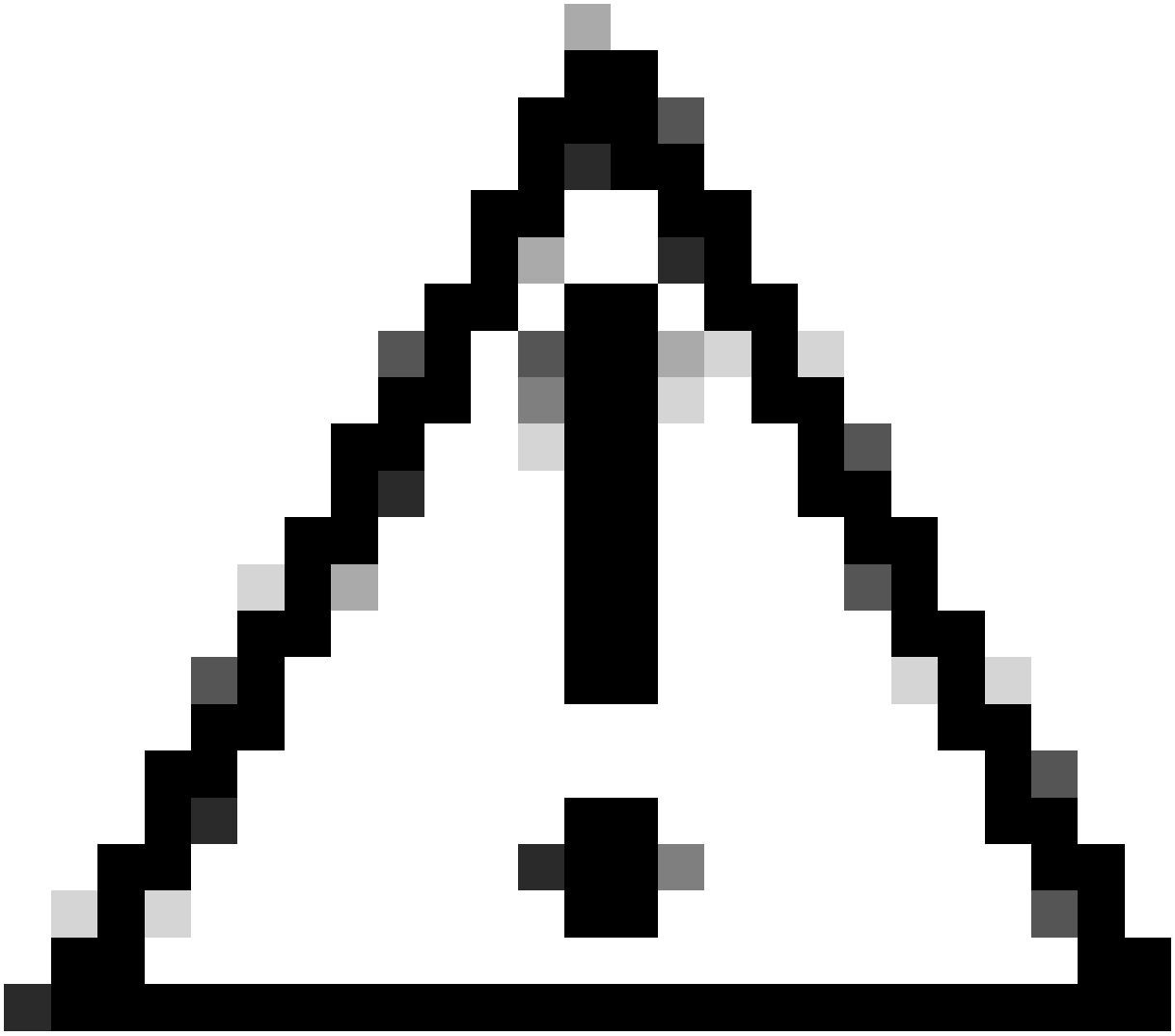
CLIを使用する場合：

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

GUIを使用する場合：DHCPセクションのConfiguration > Tags & Profile > Policy > Policy_name > Advanced. で、ipv4 DHCP requiredを有効にします。



WLCでのポリシープロファイルの設定



注意：外部アンカー設定の場合、DHCP設定を両方のWLCに合わせることが重要です。IPV4 DHCP requiredをイネーブルにしている場合は、外部WLCとアンカーWLCの両方でイネーブルにする必要があります。2つの間でポリシープロファイルの下にあるDHCP関連の設定に不一致があると、クライアントでモビリティロールに関する問題が発生する可能性があります。

問題2:IP盗用の問題により、クライアントが削除または除外される。ネットワーキングにおけるIP盗用とは、複数のワイヤレスクライアントが同じIPアドレスを使用しようとする状況を指します。これは、次に示す多くの理由が原因である可能性があります。

1. 不正な静的IPアドレスの割り当て：ユーザが静的IPアドレスをデバイスに設定し、そのアドレスがネットワーク上ですでに割り当てられているIPアドレスまたはマークされているIPアドレスと一致すると、IPアドレスの競合が発生する可能性があります。これは、2台のデバイスが同じIPアドレスで動作しようとすると発生します。これにより、関係する一方または両方のデバイスのネットワーク接続が中断される可能性があります。このような問題を防ぐには、ネットワーク上の各クライアントに一意のIPアドレスを設定することが不可欠です。

2. 不正なDHCPサーバ：ネットワーク上に不正なDHCPサーバや不正なDHCPサーバが存在すると、IPアドレスの割り当てにつながり、ネットワークの確立されたIPアドレッシング計画と衝突する可能性があります。このような競合が発生すると、複数のデバイスでIPアドレスの競合が発生したり、不適切なネットワーク設定が取得されたりする可能性があります。この問題に対処するには、不正なDHCPサーバを特定してネットワークから排除し、同じサブネット内でさらなるIP競合を防ぐ必要があります。

3. 9800 WLCでのクライアントの古いエントリ：コントローラは、クライアントが取得しようとしているIPアドレスの古い/古いエントリを保持することがあります。このような場合、9800 WLCからこれらの古いエントリを手動で削除する必要があります。その方法を次に示します。

- 除外リストに含まれるMACアドレスの放射性トレースを実行し、放射性トレース内の適切なMACでフィルタリングします。

- エラーログを確認できます。%CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON:Client MAC: Affected_Client_MAC with IP: 10.37.57.24 was added to exclusion list, legit Client MAC: Legit_Client_MAC, IP: 10.37.57.24, reason: IP address theft

- 次に、次のコマンドを実行します。
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

（古いエントリがある場合は、正規のクライアントMacアドレスに対して複数のIPを確認できます。1つは元のIPで、もう1つは古い/古いIPです。）

解決策：WLCの9800から古いエントリを手動で clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. 同じサブネットを使用するローカルDHCPサーバを使用したFlexConnectの導入：FlexConnectの設定では、さまざまなリモートロケーションが同じサブネットからIPアドレスを割り当てるローカルDHCPサーバを使用するのが一般的です。このシナリオでは、異なるサイトのワイヤレスクライアントが同じIPアドレスを受信する可能性があります。このネットワークフレームワーク内のコントローラは、複数のクライアント接続が同じIPアドレスを使用していることを検出するようにプログラムされており、これをIP盗用の可能性があると解釈します。その結果、これらのクライアントは通常、IPアドレスの競合を防ぐためにブロックされたリストに配置されます。

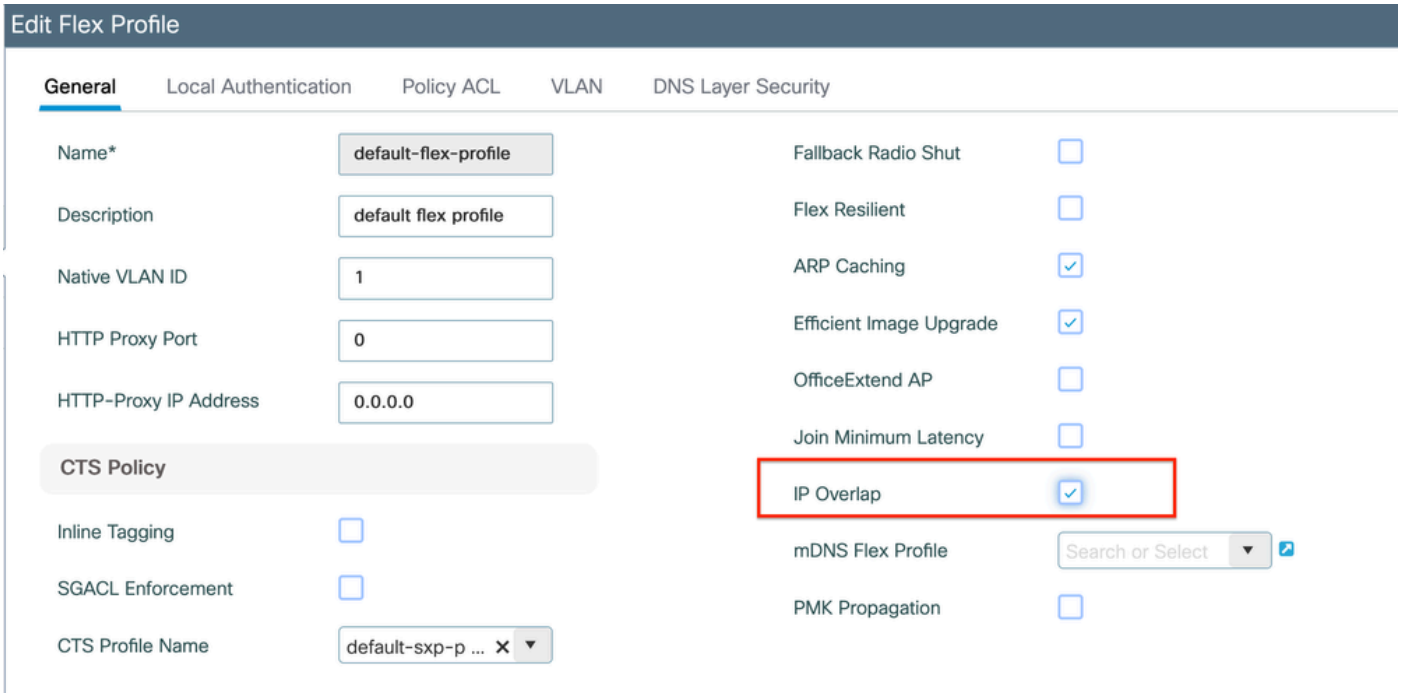
解決策：FlexConnectプロファイル内でIPオーバーラップ機能を有効にします。「Flex DeploymentでのクライアントIPアドレスの重複」機能により、FlexConnectの導入でサポートされるすべての機能を維持しながら、複数のFlexConnectサイトで同じIPアドレスを使用できます。

デフォルトでは、この機能は無効になっています。次の手順で有効にできます。

CLIを使用する場合：

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

GUIを使用：Existing Flex Profile/Add to new Flex profileをConfiguration > Tags & Profiles > Flex. クリックし、GeneralタブでIP Overlapを有効にします。



WLCでのFlexプロファイルの設定

問題 3：ワイヤレスクライアントが、対象のVLANからIPアドレスを受信できない。この問題は、VLAN 1が使用されている場合、またはクライアントに割り当てられているVLANがFlexConnectの展開でAP管理に使用されているVLANと同じ場合に頻繁に発生します。この問題の根本的な原因は、通常、VLAN割り当てが正しくないことです。ガイダンスとして、9800シリーズでVLAN IDを設定する際に考慮する必要のあるいくつかのシナリオを次に示します。

1. AAAオーバーライド機能が有効になっているAAAサーバを採用する場合、適切なVLAN IDがAAAサーバから送信されていることを確認することが重要です。代わりにVLAN名を指定する場合は、9800 WLCで設定されているVLAN名と一致することを確認します。

2. VLAN 1が無線クライアントトラフィック用に設定されている場合、動作はアクセスポイント(AP)のモードによって異なる場合があります。

ローカルモード/中央スイッチングのAP用：

- VLAN-name = defaultを指定すると、クライアントはVLAN 1に割り当てられます
- VLAN-ID 1を使用して、クライアントはワイヤレス管理VLANに割り当てられます

Flexモード/ローカルスイッチングのAPの場合：

- VLAN-name = defaultを指定すると、クライアントはVLAN 1に割り当てられます
- VLAN-ID 1を使用して、クライアントはFlexConnectネイティブVLANに割り当てられます

ラボで実験したシナリオとその結果を次に示します。

1. デフォルトでは、ユーザがポリシープロファイルで何も設定しない場合、WLCはVLAN-ID 1を割り当てます。これにより、クライアントはローカルモードでワイヤレス管理VLANを使用し、FlexConnectにはAPネイティブVLANを使用します。

2. flex-profileのネイティブVLANが、スイッチに設定されているものと異なるネイティブVLAN IDで設定されている場合、ポリシープロファイルに「default」VLAN名が設定されていても、クライアントは管理VLAN（ネイティブVLAN）からIPを取得します。

3. flex-profile上のネイティブVLANが、スイッチ上に設定されているネイティブVLANと同じVLAN-IDを使用して設定されている場合、ポリシープロファイル上でデフォルトに設定されているVLAN 1からIPを取得できるのはクライアントだけです。

4. VLAN IDではなくVLAN名を選択した場合は、Flex Profile内のVLAN名が同じであることを確認します。

関連情報

- 9800の内部DHCPサーバ
- 外部DHCPサーバが使用されている
- Windows DHCPサーバのDHCPオプション82サブオプション5
- Flex APでのNAT-PAT
- VLAN 1はワイヤレスクライアントに使用される
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。