Cisco 9800 WLC에서 DHCP 클라이언트 연결 문제 해결

목차

소개

이 문서에서는 Cisco 9800 WLC(Wireless LAN Controller)에 연결할 때 무선 클라이언트에서 발생하는 다양한 DHCP(Dynamic Host Configuration Protocol) 관련 문제와 이러한 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco WLC 9800에 대한 기본 지식
- DHCP 흐름에 대한 기본 지식

- 로컬 및 플렉스 연결 모드 AP에 대한 기본 지식

무선 클라이언트의 DHCP 트래픽 흐름 이해

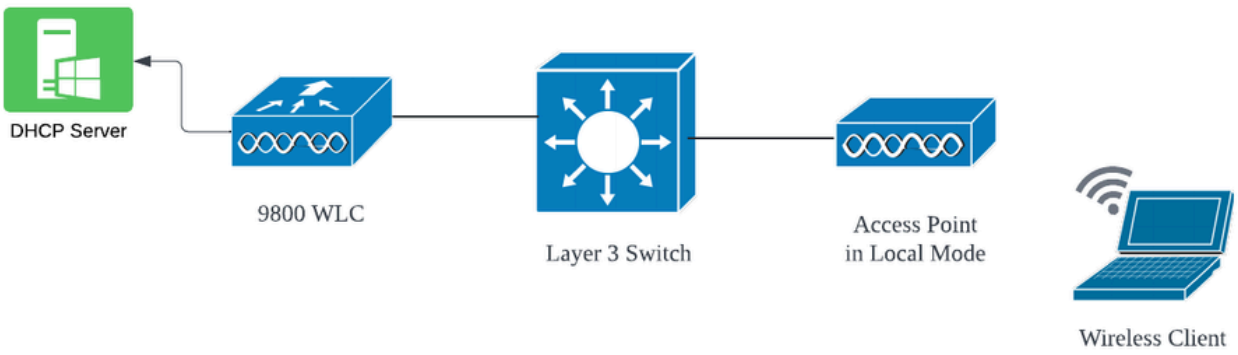
무선 클라이언트가 연결되면 브로드캐스트 DHCP 검색 프레임을 전송하여 연결된 AP에 DHCP 서버를 찾는 일반적인 DHCP 교환을 수행합니다. AP의 작동 모드에 따라 CAPWAP 터널을 통해 WLC에 요청을 전달하거나 다음 홉으로 직접 전달합니다. 로컬 레이어 2 도메인 내에서 DHCP 서버를 사용할 수 있는 경우, DHCP 서버가 응답하므로 성공적으로 연결할 수 있습니다. 로컬 서브넷 DHCP 서버가 없을 경우, DHCP 검색을 적절한 서버로 라우팅하도록 (클라이언트의 SVI로 구성된) 라우터를 설정해야 합니다. 이는 일반적으로 특정 브로드캐스트 UDP 트래픽(예: DHCP 요청)을 미리 설정된 IP 주소로 전달하도록 라우터에 IP 헬퍼 주소를 구성하는 방식으로 수행됩니다.

클라이언트 DHCP 트래픽의 동작은 전적으로 AP(액세스 포인트)가 작동 중인 모드에 따라 달라집니다. 이러한 각 시나리오를 개별적으로 살펴보겠습니다.

시나리오 1. 액세스 포인트(AP)가 로컬 모드에서 작동 중입니다.

AP가 로컬 모드로 설정되면 클라이언트 DHCP 트래픽이 중앙에서 전환됩니다. 즉, 클라이언트의 DHCP 요청이 CAPWAP 터널을 통해 AP에서 WLC로 전송되며, 이 터널에서 AP가 처리되고 그에 따라 전달됩니다. 이 경우 두 가지 선택 사항이 있습니다. 내부 DHCP 서버를 활용하거나 외부 DHCP 서버를 선택할 수 있습니다.

토폴로지(로컬 모드 AP)



네트워크 토폴로지: 로컬 모드 *AP*

사례 연구 1. WLC가 내부 DHCP 서버로 구성된 경우

컨트롤러는 Cisco IOS XE 소프트웨어의 통합 기능을 통해 내부 DHCP 서버를 제공할 수 있습니다. 그러나 외부 DHCP 서버를 사용하는 것이 모범 사례로 간주됩니다. WLC를 내부 DHCP 서버로 설정하기 전에 다음과 같은 몇 가지 전제 조건을 충족해야 합니다.

- 클라이언트 VLAN에 대해 SVI(Switched Virtual Interface)를 구성하고 DHCP 서버의 IP 주소를 할당해야 합니다.
- 내부 DHCP 서버의 IP 주소는 루프백 인터페이스, SVI 또는 레이어 3 물리적 인터페이스일 수 있는 서버 연결 인터페이스에서 설정해야 합니다.
- 루프백 인터페이스는 실제 네트워크 세그먼트에 연결하는 물리적 인터페이스와 달리 하드웨어에 연결되지 않으며 디바이스의 물리적 포트에 해당하지 않으므로 구성하는 것이 좋습니다. 루프백 인터페이스의 주요 목적은 하드웨어 장애 또는 물리적 연결이 끊기지 않는 안정적이고 항상 가동되는 인터페이스를 제공하는 것입니다.

설정 작업: 다음은 클라이언트가 성공적으로 IP 주소를 받은 내부 DHCP 서버 구성의 예입니다. 다음은 운영 로그와 관련 설정 세부 정보입니다.

VLAN 10의 DHCP 서버로 WLC를 설정합니다. DHCP 범위는 10.106.10.11/24~10.106.10.50/24입니다.

```
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
```

WLC에 구성된 루프백 인터페이스:

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

WLC에서 도우미 주소를 루프백 인터페이스로 사용하여 SVI [L3 Interface]로 구성된 클라이언트 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
```

또는 SVI 아래에서 헬퍼 주소를 구성하는 대신 정책 프로필 내에서 DHCP 서버의 IP 주소를 설정할 수 있습니다. 그러나 일반적으로 모범 사례에서는 VLAN별로 이를 구성하는 것이 좋습니다.

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

WLC의 방사선 흔적:

```
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
```

WLC의 임베디드 패킷 캡처:

```
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*의 임베디드 패킷 캡처

AP 클라이언트 디버깅:

```
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>
```

클라이언트측 패킷 캡처:

```
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
```

클라이언트 종료 패킷 캡처

제공된 운영 로그에서 WLC가 무선 클라이언트로부터 DHCP Discover 메시지를 수신하고 있으며, 클라이언트의 VLAN이 헬퍼 주소(제공된 예에서 내부 루프백 인터페이스)에 이를 릴레이하고 있음을 확인할 수 있습니다. 그 다음 내부 서버가 DHCP Offer를 발행하고, 클라이언트가 DHCP Request를 전송하면 서버가 DHCP ACK를 사용하여 이를 승인합니다.

무선 클라이언트 IP 확인:

WLC의 경우:

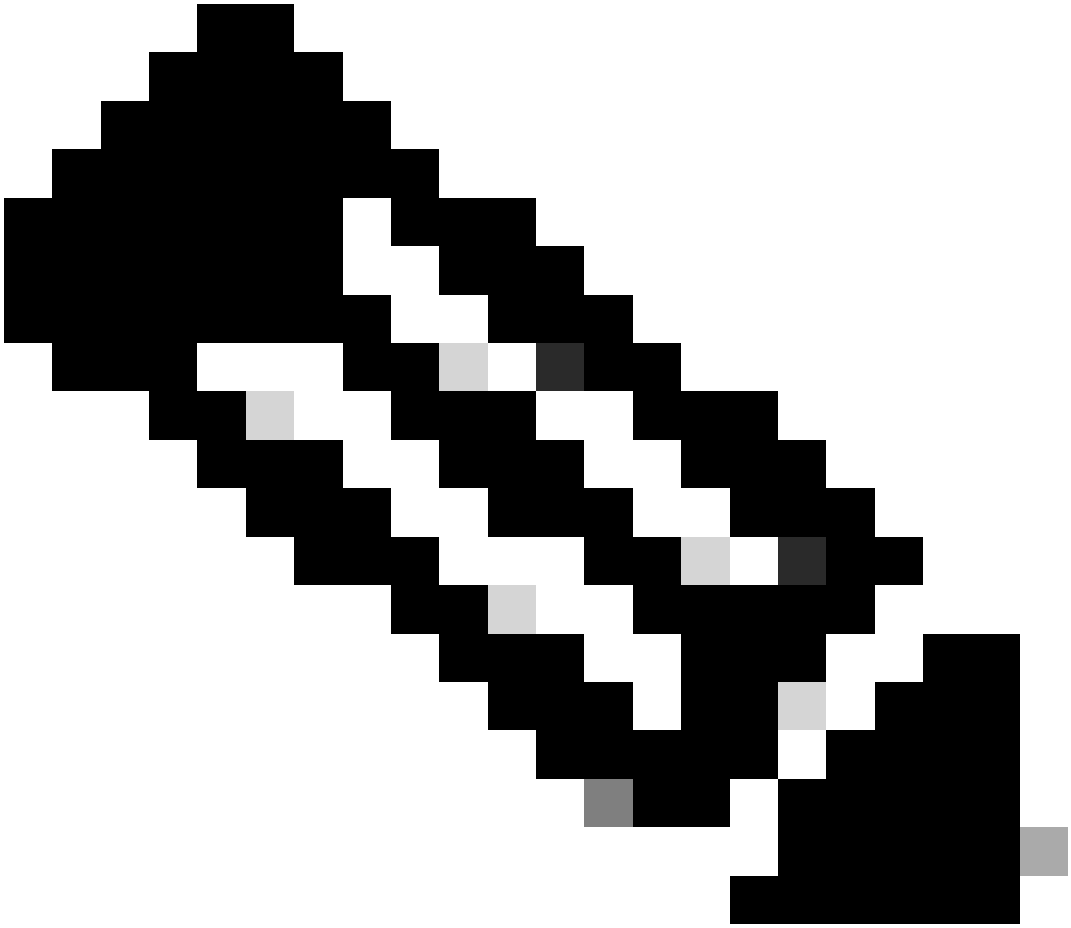
```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type          State
10.106.10.12      aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active     L
```

무선 클라이언트의 경우:

```
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
```

클라이언트 쪽에서 *IP* 확인



참고:
1. 내부 DHCP 서버에서 VRF가 지원되지 않습니다.
2. DHCPv6는 내부 DHCP 서버에서 지원되지 않습니다.

---

3. C9800에서 SVI는 여러 헬퍼 주소를 구성할 수 있지만 처음 2개만 사용됩니다.
4. 이 기능은 테스트를 거쳤으므로 모든 플랫폼에서 최대 클라이언트 확장 용량의 최대 20%까지 지원됩니다. 예를 들어, 64,000개의 클라이언트를 지원하는 9800-80의 경우 지원되는 최대 DHCP 바인딩은 약 14,000개입니다.

사례 연구 2. 외부 DHCP 서버가 사용되는 경우

외부 DHCP 서버는 WLC 자체에 통합되지 않고 다른 네트워크 장치[방화벽, 라우터]에 구성되거나 네트워크 인프라 내의 별도의 엔터티에 구성되는 DHCP 서버를 의미합니다. 이 서버는 네트워크의 클라이언트에 대한 IP 주소 및 기타 네트워크 컨피그레이션 매개변수의 동적 배포를 관리하는 데 사용됩니다.

외부 DHCP 서버를 활용할 때 WLC의 기능은 오로지 트래픽을 수신하고 릴레이하는 것입니다. DHCP 트래픽이 WLC에서 라우팅되는 방법(브로드캐스트 또는 유니캐스트)은 환경 설정에 따라 달라집니다. 이러한 각 방법을 개별적으로 고려해보자.

레이어 2 도메인을 통한 DHCP 트래픽 브로드캐스트

이 설정에서는 방화벽, 업링크 또는 코어 스위치와 같은 다른 네트워크 장치가 릴레이 에이전트 역할을 합니다. 클라이언트가 DHCP 검색 요청을 브로드캐스트할 때 WLC의 유일한 작업은 레이어 2 인터페이스를 통해 이 브로드캐스트를 전달하는 것입니다. 이 기능이 올바르게 작동하려면 클라이언트 VLAN의 레이어 2 인터페이스가 올바르게 구성되어 있고 WLC의 데이터 포트 및 업링크 디바이스를 통해 허용되는지 확인해야 합니다.

이 인스턴스의 클라이언트 VLAN 20에 대한 WLC 끝에 원하는 컨피그레이션:

WLC에 구성된 레이어 2 VLAN:

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

클라이언트 VLAN의 트래픽을 허용하도록 WLC에 데이터 포트를 구성했습니다.

```
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 WLC의 방사선 흔적:

```
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
```

9800 WLC에서 수행된 내장형 패킷 캡처:

```
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*의 임베디드 패킷 캡처

AP 클라이언트 디버깅:

```
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>
```

클라이언트 측 캡처:

```
  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
```

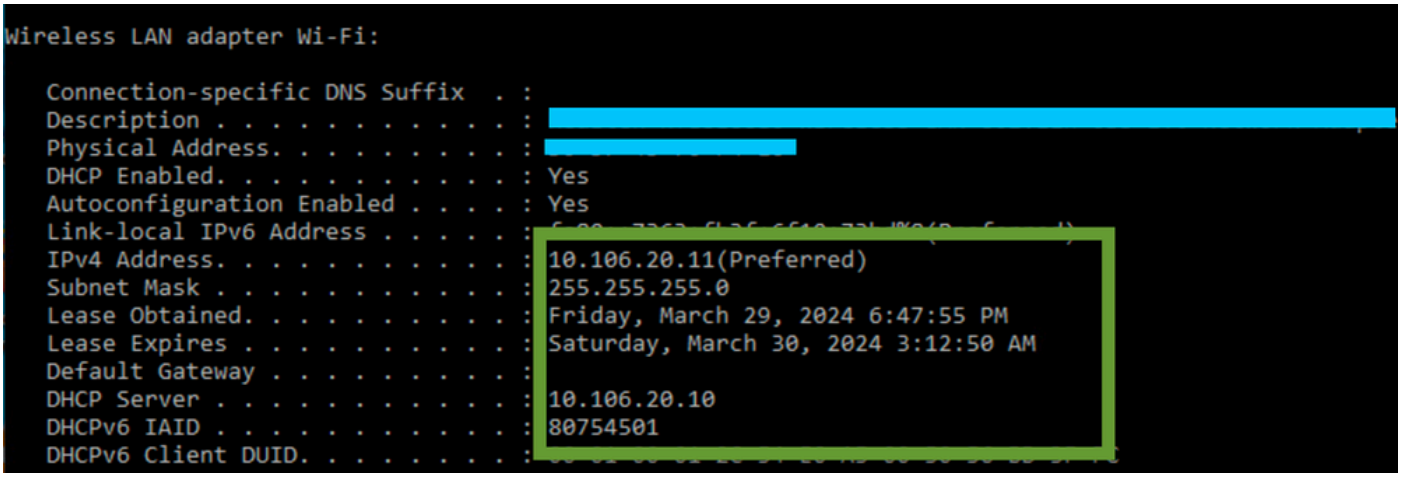
클라이언트 종료 패킷 캡처

제공된 작업 로그에서 WLC가 무선 클라이언트에서 DHCP Discover 브로드캐스트를 가로채고 있다는 것을 확인한 다음 L2 인터페이스를 통해 다음 홉으로 브로드캐스팅합니다. WLC는 서버에서 DHCP Offer를 받자마자 이 메시지를 클라이언트에 전달하고 DHCP Request 및 ACK를 전달합니다.

무선 클라이언트 IP 확인:

DHCP 서버의 IP 임대 및 해당 상태를 확인할 수 있습니다.

무선 클라이언트의 경우:



클라이언트 쪽에서 *IP* 확인

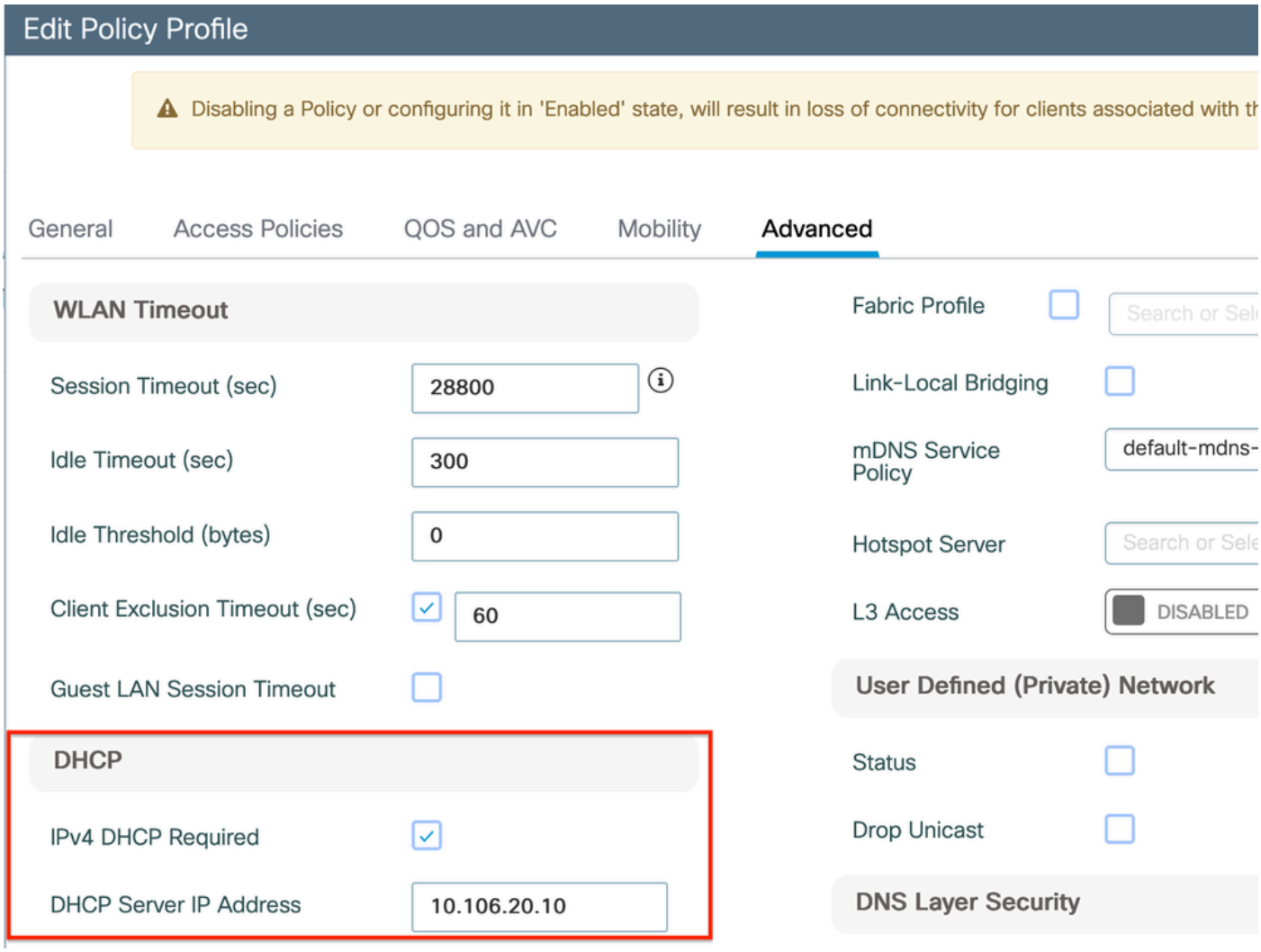
9800 WLC가 릴레이 에이전트 역할을 함

이 컨피그레이션에서 WLC는 무선 클라이언트에서 수신한 DHCP 패킷을 유니캐스트로 DHCP 서버에 직접 전달합니다. 이를 활성화하려면 클라이언트에 대한 VLAN SVI가 WLC에 구성되어 있는지 확인합니다.

9800 WLC에서 DHCP 서버 IP를 구성하는 방법에는 2가지가 있습니다.

1. 고급 설정의 정책 프로필에서 DHCP 서버 IP를 구성합니다.

GUI를 통해: DHCP 섹션 Configuration > Tags & Profile > Policy > Policy_name > Advanced. 아래에서 다음과 같이 DHCP 서버 IP를 구성할 수 있습니다.



WLC의 정책 프로파일 설정

CLI를 통해:

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

2. SVI 컨피그레이션 내에서 도우미 주소를 지정해야 합니다. 이중화를 제공하기 위해 헬퍼 주소 컨피그레이션에서 여러 DHCP 서버를 설정할 수 있습니다. 정책 프로필 내에서 각 WLAN에 대한 DHCP 서버 주소를 설정할 수 있지만 권장되는 방법은 인터페이스별로 구성하는 것입니다. 이 작업은 해당 SVI에 헬퍼 주소를 할당하여 수행할 수 있습니다.

릴레이 기능을 사용할 때 DHCP 트래픽의 소스는 클라이언트 SVI(Switched Virtual Interface)의 IP 주소입니다. 그런 다음 이 트래픽은 라우팅 테이블에 의해 결정된 대상(DHCP 서버의 IP 주소)에 해당하는 인터페이스를 통해 라우팅됩니다.

다음은 릴레이 에이전트 역할을 하는 9800의 작업 컨피그레이션 샘플입니다.

헬퍼 주소를 사용하여 WLC의 클라이언트 VLAN에 대해 구성된 레이어 3 인터페이스:

```
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
```

클라이언트 VLAN의 트래픽을 허용하도록 WLC에 데이터 포트를 구성했습니다.

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

WLC에서 RA 추적:

```
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
```

WLC의 임베디드 패킷 캡처:

No.	Time	Source	Destination	Protocol	Length	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

WLC의 임베디드 패킷 캡처

WLC의 RA(Radioactive Traces) 및 EPC(Embedded Packet Capture) 모두에서 릴레이 에이전트 역할을 하는 WLC가 클라이언트에서 DHCP 서버로 DHCP 패킷을 직접 유니캐스팅하고 있음을 알 수 있습니다.

AP 클라이언트 디버깅:

```
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>
```

클라이언트 측 캡처:

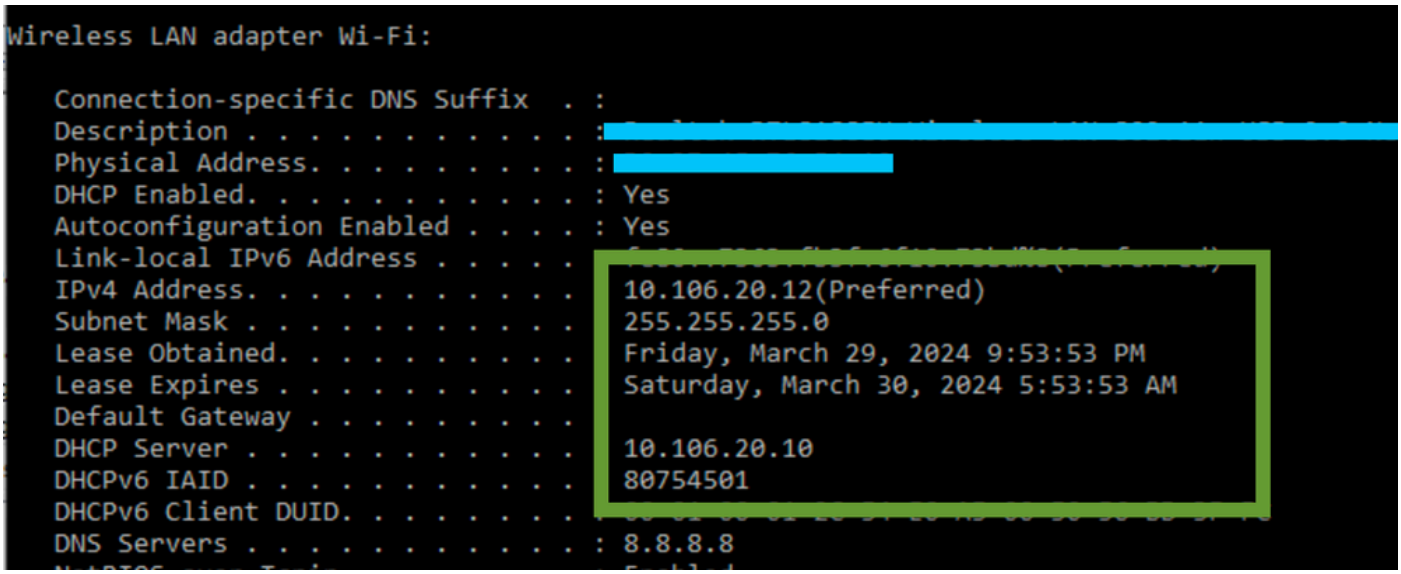
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - 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

클라이언트 종료 패킷 캡처

무선 클라이언트 IP 확인:

DHCP 서버의 IP 임대 및 해당 상태를 확인할 수 있습니다.

무선 클라이언트의 경우:



클라이언트 쪽에서 *IP* 확인

9800 WLC의 서브스크립션 5/150이 포함된 DHCP 옵션 80

특정 시나리오에서는 잠재적인 네트워크 복잡성을 방지하기 위해 라우팅 테이블에 의존하기보다는 DHCP 트래픽에 대한 소스 인터페이스를 명시적으로 정의하는 것을 선호할 수 있습니다. 이는 특히 경로를 따르는 다음 네트워크 디바이스(예: 레이어 3 스위치 또는 방화벽)에서 RPF(Reverse Path Forwarding) 검사를 사용하는 경우에 유용합니다. 예를 들어, 클라이언트 SVI가 VLAN 20에 있고 클라이언트 트래픽을 위한 DHCP 릴레이로 사용되는 동안 무선 관리 인터페이스가 VLAN 50에 설정되는 상황을 예로 들어 보겠습니다. 기본 경로는 무선 관리 VLAN/서브넷의 게이트웨이로 향합니다.

9800 WLC의 버전 17.03.03부터 DHCP 트래픽의 소스 인터페이스를 클라이언트 VLAN 또는 DHCP 서버와의 연결을 보장하는 WMI(Wireless Management Interface)와 같은 다른 VLAN으로 선택할 수 있습니다.

컨피그레이션의 스닙은 다음과 같습니다.

```
!
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
```

이 시나리오에서 DHCP 서버 10.100.17.14에 대한 트래픽은 VLAN 50(10.100.16.10)에서 소싱됩니다. 패킷의 종료 인터페이스는 IP 라우팅 테이블의 조회를 기반으로 선택되며, 일반적으로 구성된 기본 경로로 인해 WMI(Wireless Management Interface) VLAN을 통해 종료됩니다.
그러나 업링크 스위치가 RPF(Reverse Path Forwarding) 확인을 구현하는 경우 VLAN 50에서 도착하는 패킷을 버릴 수 있지만 IP 소스 주소가 다른 서브넷[VLAN 20]에 속해 있습니다.

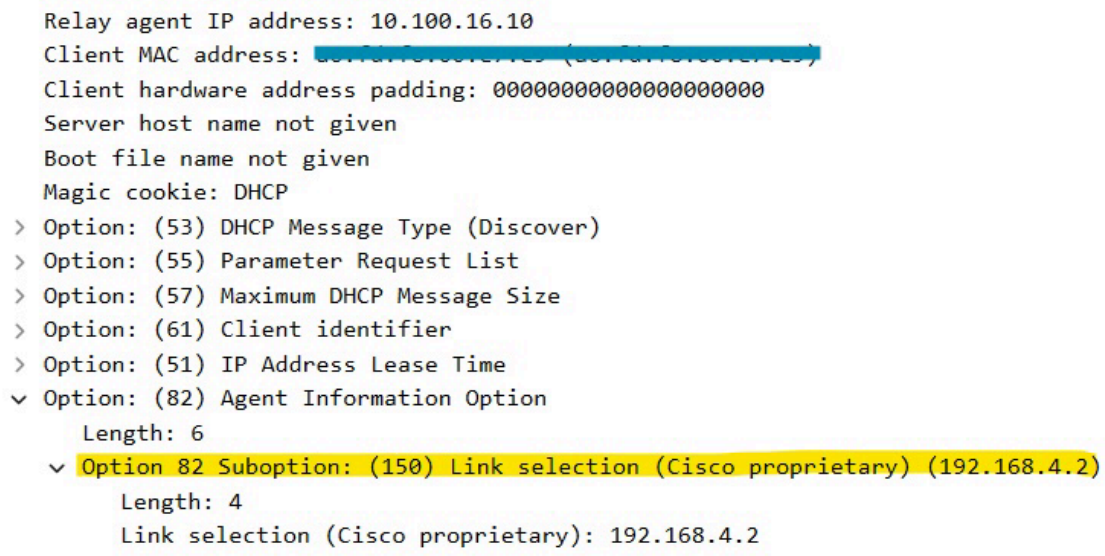
이를 방지하려면 IP DHCP relay source-interface 명령을 사용하여 DHCP 패킷의 정확한 소스 인터페이스를 설정해야 합니다. 이 경우 VLAN 50의 WMI 인터페이스에서 DHCP 패킷을 시작하도록 할 수 있습니다.

```
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
```

명령을 사용할ip dhcp relay source-interface 경우 DHCP 패킷의 소스 인터페이스 및 GIADDR이 모두 DHCP 릴레이 명령에 지정된 인터페이스(이 경우 VLAN50)로 설정됩니다. 이는 DHCP 주소를 할당하려는 클라이언트 VLAN이 아니므로 문제가 됩니다.

DHCP 서버는 올바른 클라이언트 풀에서 IP를 할당하는 방법을 어떻게 알고 있습니까?

따라서 이에 대한 대답은 명령이 사용될 때 C9800ip dhcp relay source-interface 은 캡처에서 볼 수 있듯이 링크 선택이라고 하는 옵션 82의 전용 하위 옵션 150에 클라이언트 서브넷 정보를 자동으로 추가한다는 것입니다.



옵션 182 서브스크립션 *WLC* 패킷 캡처의 150

기본적으로 하위 옵션 150(cisco 전용)이 추가됩니다. 사용된 DHCP 서버가 이 정보를 해석하고 작동할 수 있는지 확인합니다. 권장 사항은 C9800 컨피그레이션을 변경하여 표준 옵션 82, 하위 옵션 5를 사용하여 링크 선택 정보를 전송하는 것입니다. 다음 전역 명령을 구성하여 이 작업을 수행할 수 있습니다.

<#root>

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

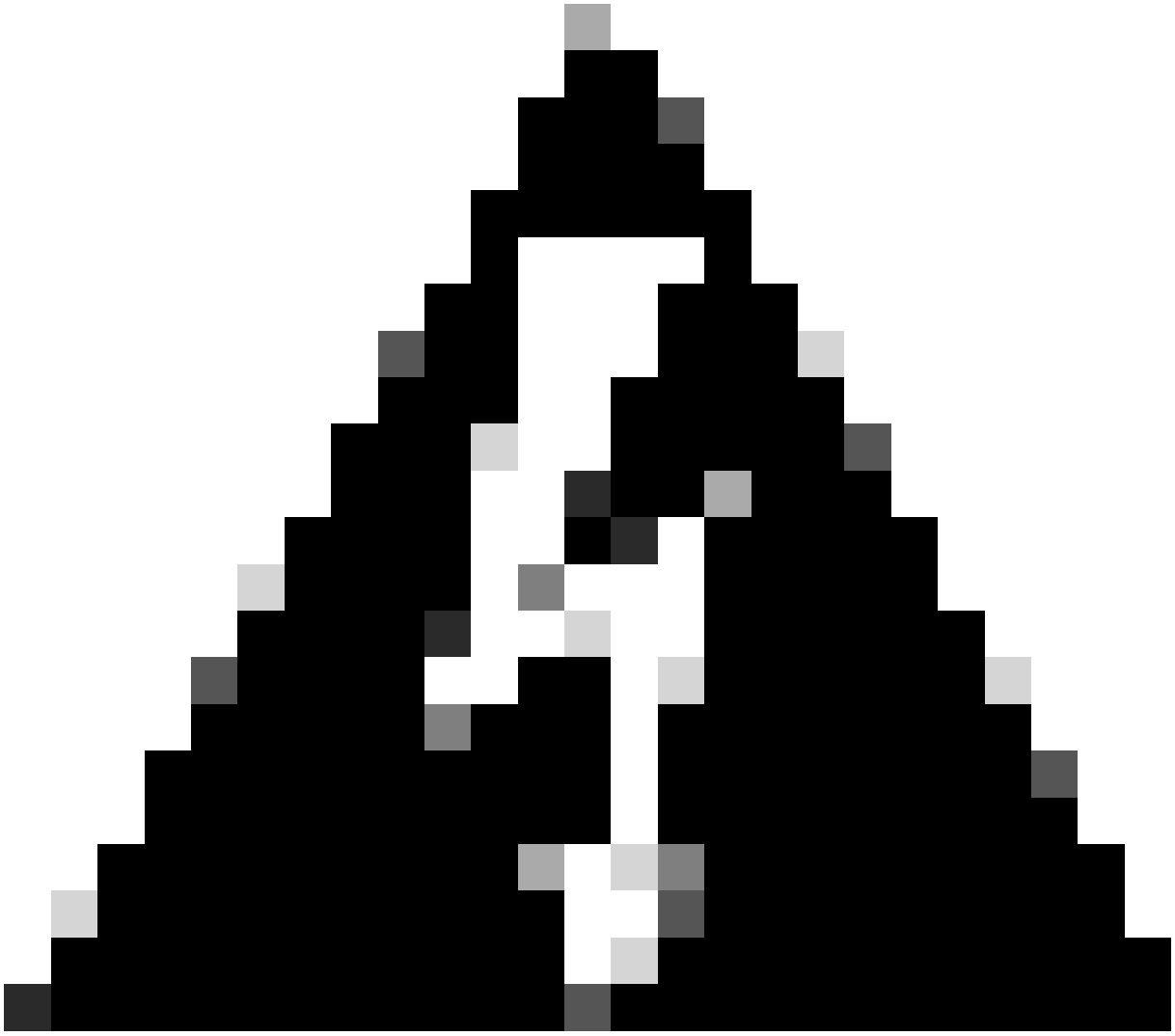
지정된 명령이 적용되면 시스템은 DHCP 패킷에서 서브스크립션 150을 서브스크립션 5로 교체합니다. 서브스크립션 5는 네트워크 디바이스에서 더 널리 인식되므로 패킷이 삭제될 가능성이 낮습니다. 이 변경 사항의 적용은 제공된 캡처에서도 분명합니다.

```
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)
```

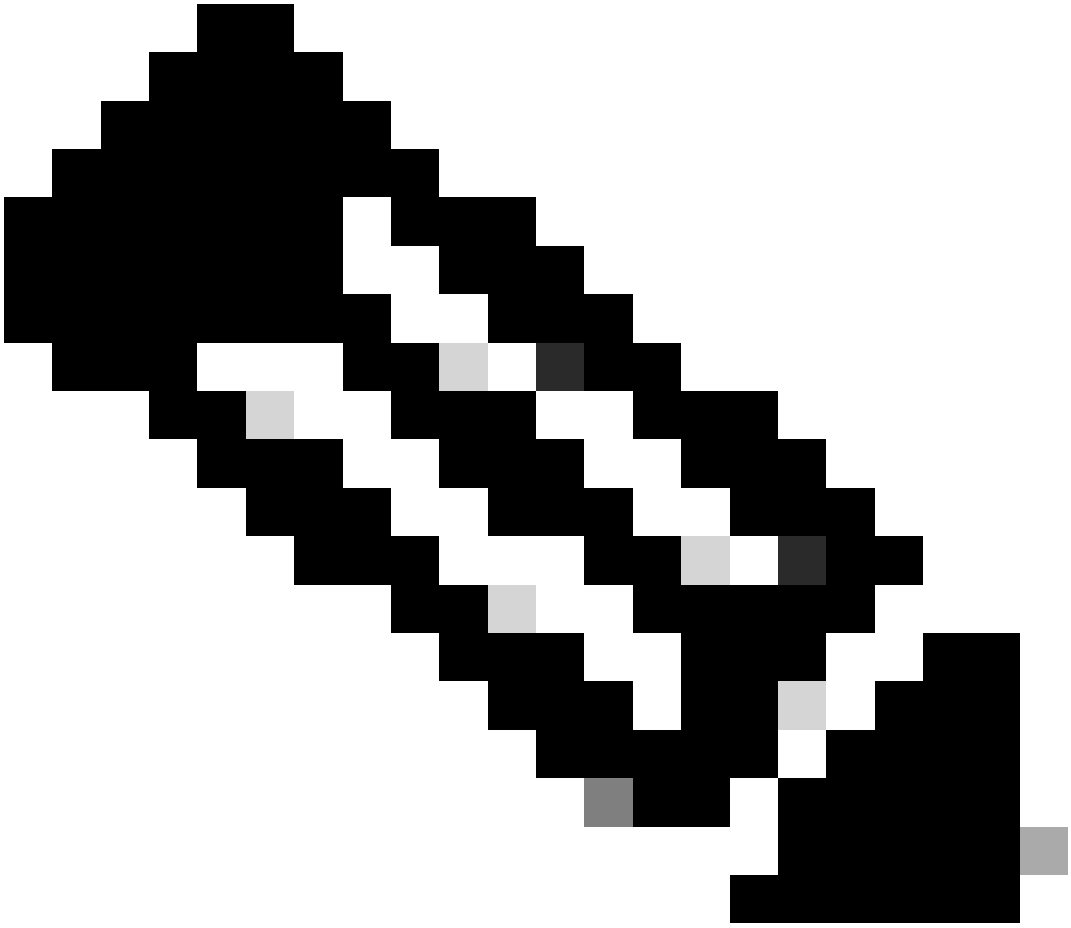
WLC 패킷 캡처의 옵션 182 하위 옵션 5

하위 옵션 5를 구현하면 DHCP 트래픽을 다른 네트워크 디바이스에서 승인해야 합니다. 그러나 특히 Windows DHCP 서버가 사용 중일 때는 여전히 NAK(부정 확인 응답) 메시지가 나타날 수 있습니다. DHCP 서버가 소스 IP 주소를 인증하지 않았기 때문일 수 있습니다. 해당 소스 IP에 대해 해당 컨피그레이션이 없기 때문일 수 있습니다.

DHCP 서버에서 해야 할 일 Windows DHCP 서버의 경우 릴레이 에이전트의 IP를 인증하기 위한 더미 범위를 만들어야 합니다.



경고: 모든 릴레이 에이전트 IP 주소(GIADDR)는 활성 DHCP 범위 IP 주소 범위에 속해야 합니다. DHCP 범위 IP 주소 범위를 벗어난 모든 GIADDR은 비인가 릴레이로 간주되며 Windows DHCP Server는 이러한 릴레이 에이전트의 DHCP 클라이언트 요청을 승인하지 않습니다. 릴레이 에이전트에 권한을 부여하기 위해 특수 범위를 생성할 수 있습니다. GIADDR으로 범위를 생성하고(또는 GIADDR이 순차적 IP 주소인 경우 여러 개), 배포에서 GIADDR 주소를 제외한 다음 범위를 활성화합니다. 이렇게 하면 릴레이 에이전트에 권한을 부여하면서 GIADDR 주소를 할당할 수 없게 됩니다.

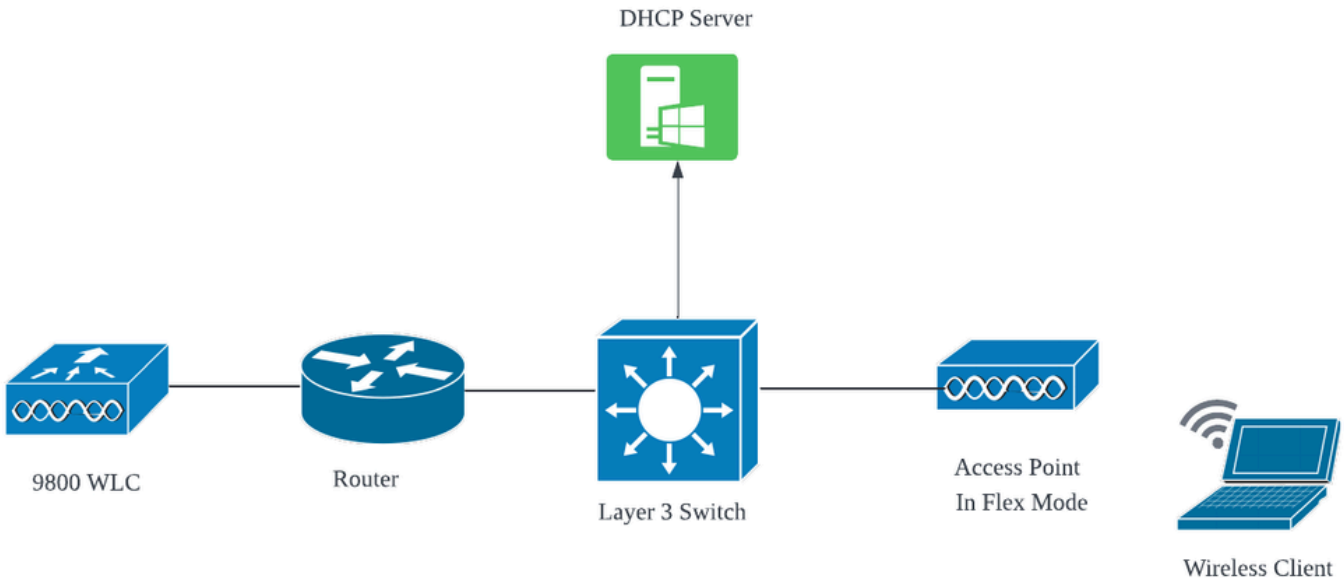


참고: 외부 앵커 설정에서 DHCP 트래픽은 AP 모드를 로컬로 설정하여 중앙에서 처리됩니다. 초기에 DHCP 요청은 외부 WLC로 전송되며, 그런 다음 모빌리티 터널을 통해 앵커 WLC로 전달됩니다. 구성된 설정에 따라 트래픽을 처리하는 앵커 WLC입니다. 따라서 DHCP와 관련된 모든 컨피그레이션은 앵커 WLC에서 구현되어야 합니다.

시나리오 2. 액세스 포인트(AP)가 Flex 모드로 작동 중입니다.

FlexConnect AP는 지사 및 원격 사무실용으로 설계되어 중앙 WLC(Wireless LAN Controller)에 대한 연결이 끊어질 경우 독립형 모드로 작동할 수 있습니다. FlexConnect AP는 트래픽을 WLC에 백홀하지 않고도 클라이언트와 네트워크 간에 트래픽을 로컬로 스위칭할 수 있습니다. 따라서 레이턴시가 줄어들고 WAN 대역폭이 절약됩니다. 플렉스 모드 AP에서는 DHCP 트래픽을 중앙에서 스위칭하거나 로컬에서 스위칭할 수 있습니다.

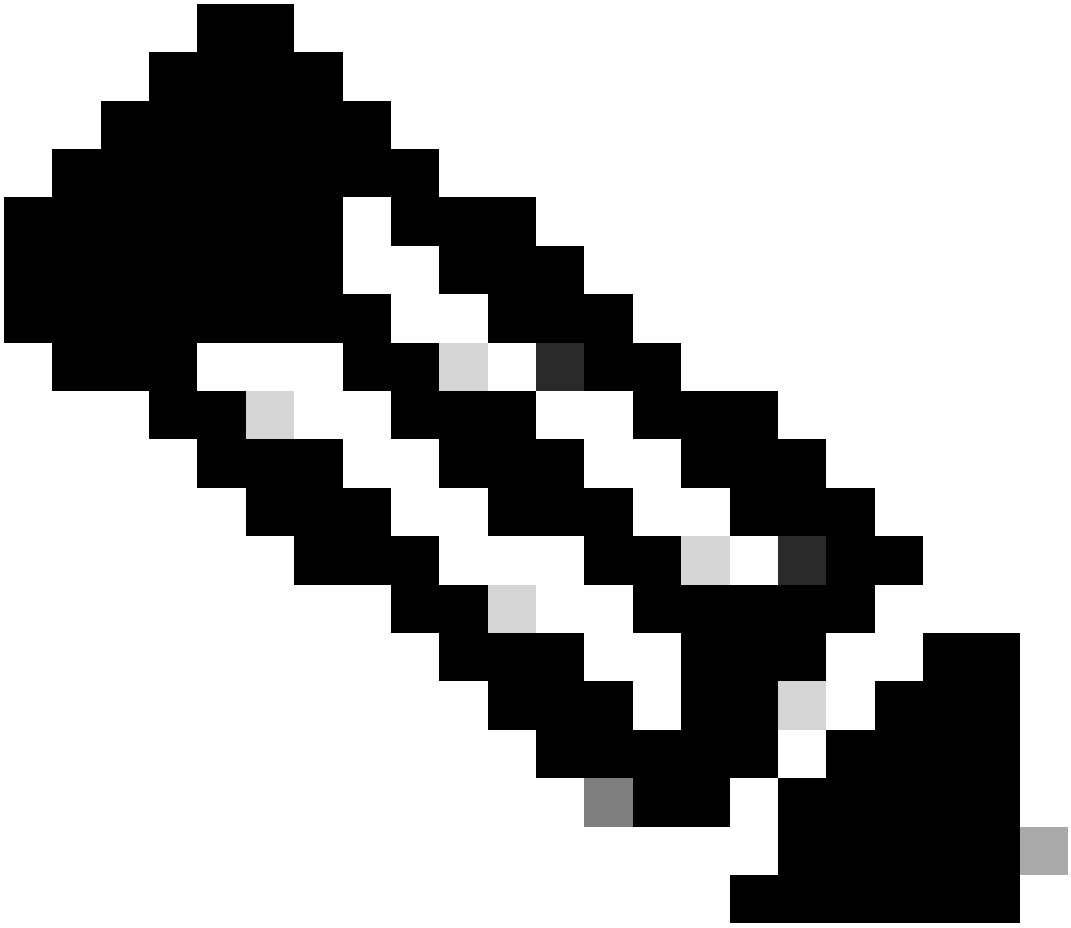
토폴로지(Flex Mode AP)



네트워크 토폴로지: *Flex Mode AP*

중앙 DHCP를 사용하는 FlexConnect 모드 AP

AP 모드에 관계없이 중앙 DHCP 서버를 사용할 때 컨피그레이션, 운영 흐름 및 문제 해결 단계는 일관되게 유지됩니다. 그러나 FlexConnect 모드의 AP의 경우 로컬 사이트에 클라이언트 SVI를 설정하지 않은 경우 일반적으로 로컬 DHCP 서버를 사용하는 것이 좋습니다.



참고: 원격 사이트에 사용 가능한 클라이언트 서브넷이 없는 경우 FlexConnect NAT-PAT를 활용할 수 있습니다. FlexConnect NAT/PAT는 AP에 연결된 클라이언트에서 발생하는 트래픽에 대해 NAT(Network Address Translation)를 수행하여 AP의 관리 IP 주소에 매핑합니다. 예를 들어, 원격 브랜치에 FlexConnect 모드로 작동하는 AP가 있고 연결된 클라이언트가 컨트롤러가 있는 본사에 있는 DHCP 서버와 통신해야 하는 경우 정책 프로필의 중앙 DHCP 설정과 함께 FlexConnect NAT/PAT를 활성화할 수 있습니다.

로컬 DHCP를 사용하는 FlexConnect 모드 AP

FlexConnect AP가 로컬 DHCP를 사용하도록 구성된 경우 AP와 연결된 클라이언트 디바이스는 동일한 로컬 네트워크 내에서 사용 가능한 DHCP 서버로부터 IP 주소 컨피그레이션을 수신합니다. 이 로컬 DHCP 서버는 라우터, 전용 DHCP 서버 또는 로컬 서브넷 내에서 DHCP 서비스를 제공하는 기타 네트워크 디바이스일 수 있습니다. 로컬 DHCP를 사용하면 DHCP 트래픽이 로컬 네트워크 내에서 전환됩니다. 즉, AP가 클라이언트에서 DHCP 요청을 직접 인접 홉(예: 액세스 스위치)으로 릴레이합니다. 여기서 요청은 네트워크 구성에 따라 처리됩니다.

사전 요구 사항:

1. FlexConnect 가이드를 참조하여 컨피그레이션이 가이드에 설명된 지침 및 모범 사례와 일치하는지 확인하십시오.

2. 클라이언트 VLAN은 flex profile 아래에 나열되어야 합니다.
3. AP 관리 VLAN을 기본 VLAN으로 지정하여 AP를 트렁크 모드로 설정하고, 클라이언트 트래픽에 대한 VLAN을 트렁크에서 허용해야 합니다.

다음은 관리 VLAN이 58이고 클라이언트 VLAN이 20인 AP 연결 switchport 컨피그레이션의 예입니다.

```
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
!
```

작업 설정: AP가 Flex 모드로 구성된 경우 로컬 DHCP 서버와 운영 로그를 공유하는 방법에 대한 참조:

AP 클라이언트 디버깅:

```
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 업링크 캡처:

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 업링크 캡처

클라이언트 측 캡처:

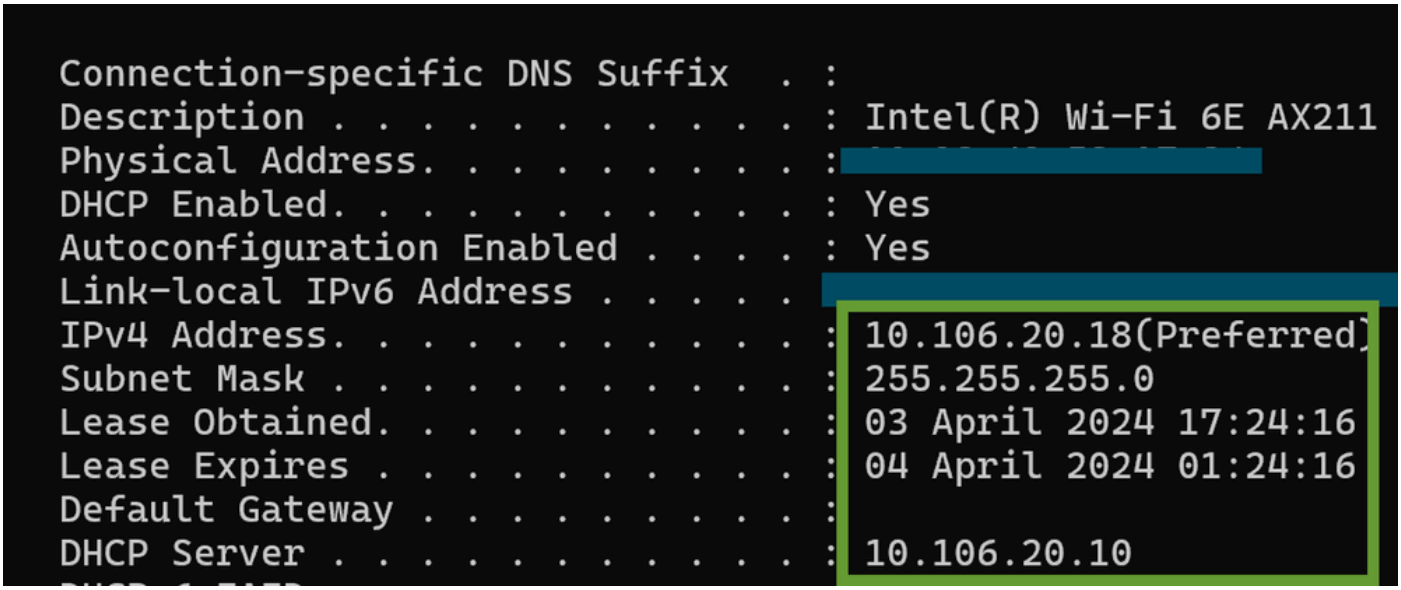
```
16540 111.905836    0.0.0.0          255.255.255.255    DHCP     343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18       DHCP     342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255    DHCP     385 DHCP Request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

클라이언트 종료 패킷 캡처

무선 클라이언트 IP 확인:

DHCP 서버의 IP 임대 및 해당 상태를 확인할 수 있습니다.

무선 클라이언트의 경우:



클라이언트 쪽에서 *IP* 확인

DHCP 문제 해결

DHCP 문제 해결에는 클라이언트가 무선 네트워크에 연결되어 있을 때 DHCP 서버에서 IP 주소를 가져올 수 없는 문제를 식별하고 해결하는 작업이 포함됩니다. 다음은 DHCP 문제를 해결할 때 몇 가지 일반적인 단계와 고려 사항입니다.

1. 클라이언트 구성 확인

- 클라이언트가 IP 주소를 자동으로 가져오도록 구성되었는지 확인합니다.
- 네트워크 어댑터가 활성화되어 있고 제대로 작동하는지 확인합니다.

2. DHCP 서버 상태 확인

- DHCP 서버가 작동 중이며 클라이언트의 네트워크 세그먼트에서 연결할 수 있는지 확인합니다.
- DHCP 서버의 IP 주소, 서브넷 마스크 및 기본 게이트웨이 설정을 확인합니다.

3. 범위 구성 검토

- DHCP 범위가 클라이언트에 사용 가능한 충분한 IP 주소 범위를 가지고 있는지 검사합니다.
- 범위의 임대 기간 및 옵션(예: DNS 서버 및 기본 게이트웨이)을 확인합니다.
- 일부 환경(예: Active Directory)에서는 DHCP 서버가 네트워크 내에서 DHCP 서비스를 제공할 권한이 있는지 확인합니다.

4. 9800 WLC의 컨피그레이션 검토

- 루프백 인터페이스 누락, 클라이언트 SVI 또는 구성된 헬퍼 주소의 부재와 같은 컨피그레이션 오류로 인해 많은 문제가 발생했습니다. 로그를 수집하기 전에 컨피그레이션이 올바르게 구현되었는지 확인하는 것이 좋습니다.
- 내부 DHCP 서버 사용 시: DHCP 범위 소진과 관련하여, 특히 CLI를 통해 DHCP를 구성할 때 임대 타이머가 요구 사항에 따라 구성되었는지 확인하는 것이 중요합니다. 기본적으로 임대 타이머는 9800 WLC에서 infinite로 설정됩니다.
- 중앙 DHCP 서버를 사용할 때 WLC 업링크 포트에서 클라이언트 VLAN 트래픽이 허용되는지 확인합니다. 반대로, 로컬 DHCP 서버를 사용할 경우 AP 업링크 포트에서 관련 VLAN이 허용되는지 확인합니다.

5. 방화벽 및 보안 설정

- 방화벽 또는 보안 소프트웨어가 DHCP 트래픽을 차단하지 않는지 확인합니다(DHCP 서버의 경우 포트 67, DHCP 클라이언트의 경우 포트 68).

로그 수집

WLC에서 로그

1. 모든 명령에 대한 시간 참조를 포함하려면 term exec 프롬프트 타임스탬프를 활성화합니다.

2. 컨피그레이션을 검토하는 데 사용합니다show tech-support wireless !! .

2. 클라이언트 수, 클라이언트 상태 분포 및 제외된 클라이언트를 확인할 수 있습니다.
show wireless summary !! 총 AP 및 클라이언트 수
show wireless exclusionlist !! 고객이 제외된 것으로 보이는 경우
show wireless exclusionlist client mac-address MAC@ !! 제외된 구체적인 클라이언트에 대한 자세한 내용을 확인하고 그 이유가 클라이언트에 대한 IP 도용으로 나열되어 있는지 확인합니다.

3. 클라이언트에 대한 IP 주소 할당을 확인하거나, 잘못된 주소 또는 예기치 않은 고정 주소 학습, DHCP 서버의 응답이 없어 더티(dirty)로 표시된 VLAN 또는 DHCP/ARP를 처리하는 SISF의 패킷 삭제를 확인합니다.

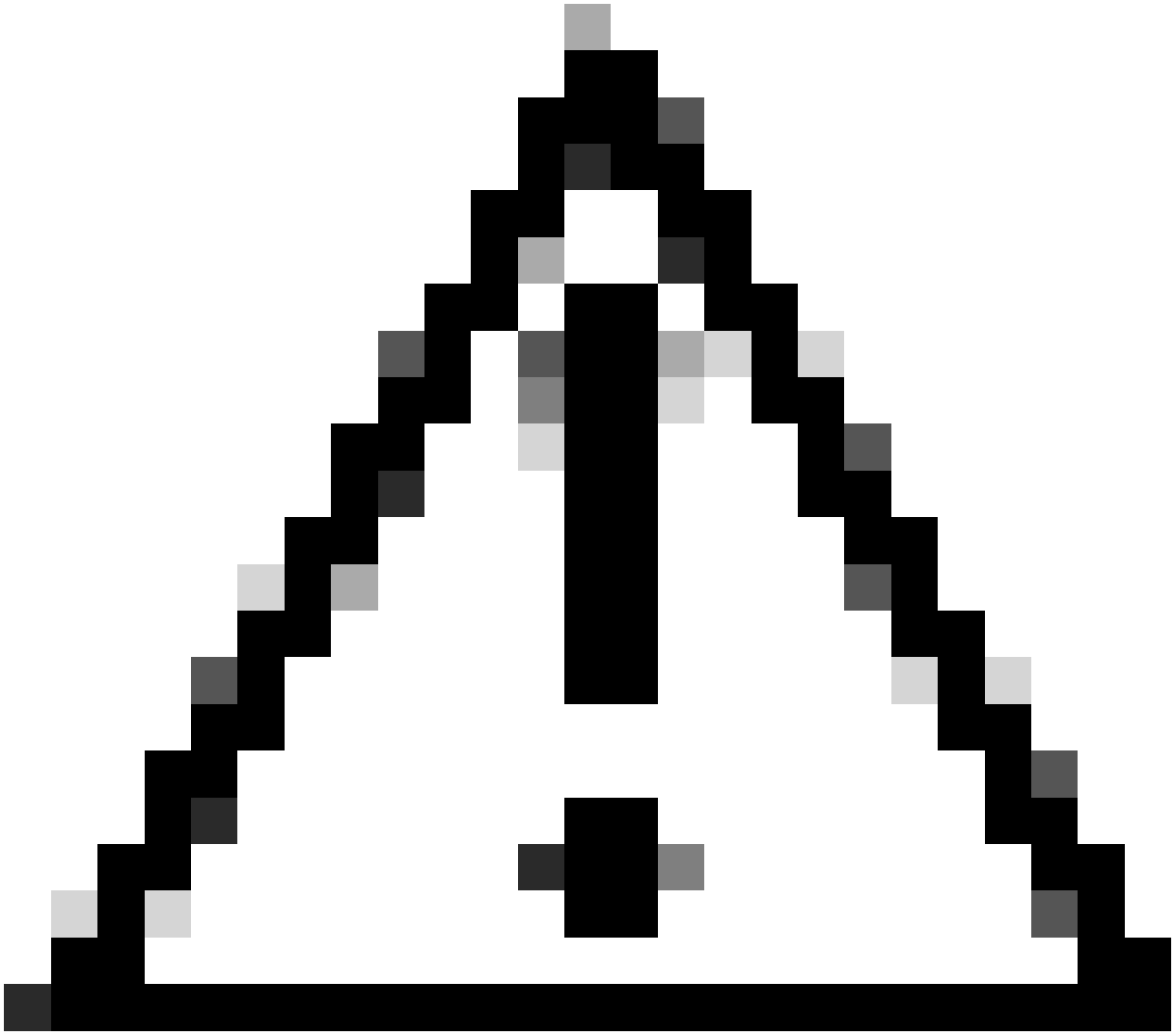
show wireless device-tracking database ip !! IP로 확인하여 주소 학습이 어떻게 이루어졌는지 확인합니다.
show wireless device-tracking database mac !! Mac에서 확인하고 어떤 IP 클라이언트가 할당되었는지 확인합니다.
show wireless vlan details !! 사용 중인 VLAN 그룹의 경우 DHCP 실패로 인해 VLAN이 더티(dirty)로 표시되지 않는지 확인합니다.
show wireless device-tracking feature drop !!SISF에서 삭제

4. 구체적인 클라이언트 MAC@에 대한 WLC의 특정 출력 show wireless device-tracking feature drop

클라이언트가 무선 네트워크에 연결하려고 할 때 클라이언트 MAC 주소에 대한 방사성 추적을 활성화합니다.

CLI를 통해:

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



주의: 조건부 디버깅은 디버그 레벨 로깅을 활성화하므로 생성된 로그의 볼륨이 증가합니다. 이 작업을 계속 실행하면 로그를 볼 수 있는 시간이 줄어듭니다. 따라서 트러블슈팅 세션이 끝날 때 항상 디버깅을 비활성화하는 것이 좋습니다.

모든 디버깅을 비활성화하려면 다음 명령을 실행합니다.

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

GUI를 통해:

1단계. 탐색 Troubleshooting > Radioactive Trace .

2단계. 를 클릭하고 Add 문제를 해결할 클라이언트 Mac 주소를 입력합니다. 추적할 여러 Mac 주소를 추가할 수 있습니다.

3단계. 방사능 추적을 시작할 준비가 되면 start(시작)를 클릭합니다. 일단 시작되면, 추적 된 MAC 주소와 관련된 제어 평면 처리에 대한 디버깅 로깅은 디스크에 기록됩니다.

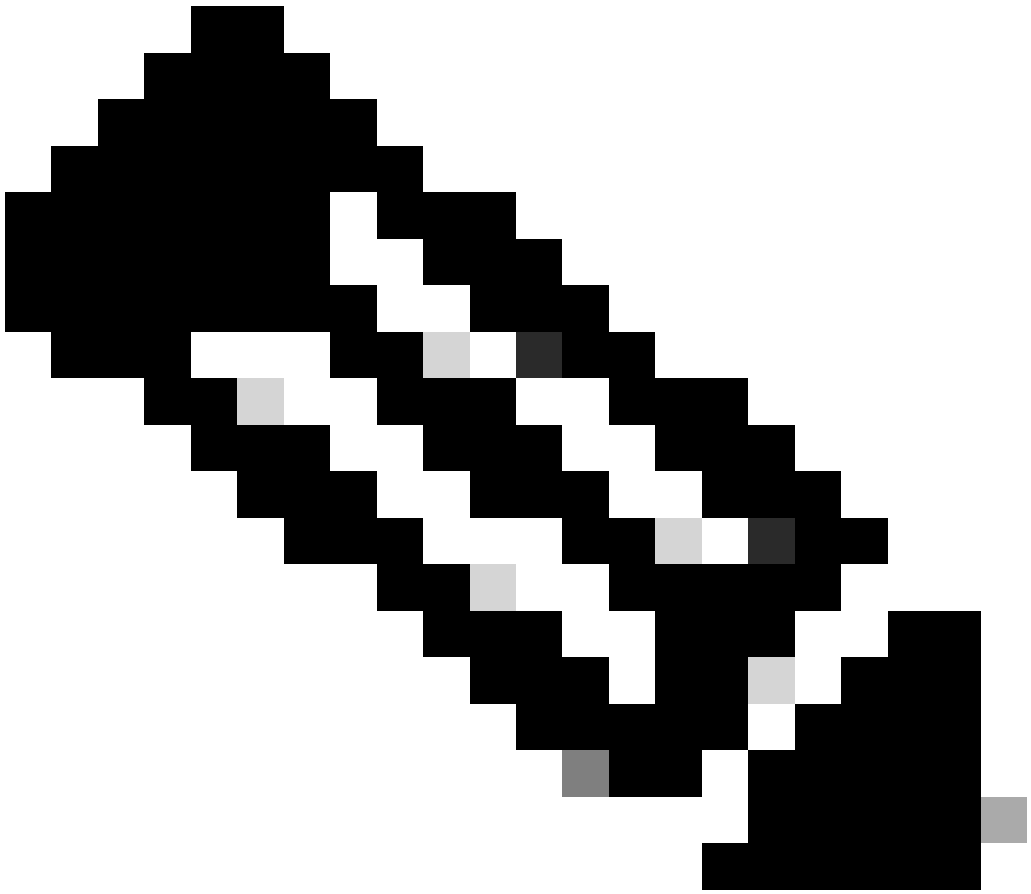
4단계. 트러블슈팅할 문제를 재현하면 을 클릭합니다Stop.

5단계. 디버깅된 각 mac 주소에 대해 을 클릭하여 해당 mac 주소와 관련된 모든 로그를 취합하는 로그 파일을 생성할 수 Generate 있습니다.

6단계. 취합된 로그 파일을 저장할 기간을 선택하고 Apply to Device(디바이스에 적용)를 클릭합니다.

7단계. 이제 파일 이름 옆에 있는 작은 아이콘을 클릭하여 파일을 다운로드할 수 있습니다. 이 파일은 컨트롤러의 부트 플래시 드라이브에 있으며 CLI를 통해 즉시 복사할 수도 있습니다.

!!클라이언트 MAC 주소로 양방향으로 필터링된 임베디드 캡처, 17.1 이후 사용 가능한 클라이언트 내부 MAC 필터.



참고: 9800의 EPC는 9800 WLC에서 중앙 DHCP가 활성화된 경우 유용합니다.

CLI를 통해:

```
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
```

GUI를 통해:
1단계. 로 Troubleshooting > Packet Capture > +Add 이동합니다.

2단계. 패킷 캡처의 이름을 정의합니다. 최대 8자까지 허용됩니다.

3단계. 필터를 정의합니다(있는 경우).

4단계. 시스템 CPU로 보내지고 데이터 플레인으로 다시 주입되는 트래픽을 보려면 Monitor Control Traffic(제어 트래픽 모니터링) 확인란을 선택합니다.

5단계. 버퍼 크기를 정의합니다. 최대 100MB가 허용됩니다.

6단계. 원하는 대로 1~1000000초 범위를 허용하는 기간 또는 1~100000 패킷 범위를 허용하는 패킷 수로 제한을 정의합니다.

7단계. 왼쪽 열의 인터페이스 목록에서 인터페이스를 선택하고 화살표를 선택하여 오른쪽 열로 이동합니다.

8단계. 저장 후 장치에 적용합니다.

9단계. 캡처를 시작하려면 Start(시작)를 선택합니다.

10단계. 캡처가 정의된 한도까지 실행되도록 할 수 있습니다. 캡처를 수동으로 중지하려면 중지를 선택합니다.

11단계. 중지되면 내보내기 버튼을 클릭하여 HTTP 또는 TFTP 서버 또는 FTP 서버나 로컬 시스템 하드 디스크 또는 플래시를 통해 로컬 데스크톱에 캡처 파일(.pcap)을 다운로드할 수 있습니다.

AP측의 로그

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

DHCP 서버의 로그

외부 DHCP 서버를 사용할 경우 DHCP 트래픽의 흐름을 확인하기 위해 서버 측에서 디버그 로그와 패킷 캡처를 수집해야 합니다.

기타 로그

중앙 DHCP 설정의 9800 WLC 또는 로컬 DHCP 설정의 AP 디버그 로그에 DHCP 검색 메시지가 표시되는 경우, 업링크에서 캡처 데이터를 수집하여 패킷이 이더넷 포트에서 삭제되지 않는지 확인해야 합니다. 스위치의 기능에 따라 업링크 스위치에서 임베디드 패킷 캡처 또는 SPAN(Switched Port Analyzer) 캡처를 수행할 수 있습니다. DHCP 클라이언트에서 DHCP 서버로, 그리고 반대 방향으로 통신이 중단된 지점을 확인하려면 DHCP 트래픽 흐름을 단계별로 추적하는 것이 좋습니다.

알려진 문제

문제 1. 클라이언트가 이전에 보유했던 VLAN에서 IP 주소를 가져오려고 합니다. 무선 클라이언트가 서로 다른 클라이언트 VLAN과 연결된 두 SSID 사이를 전환하는 상황이 발생할 수 있습니다. 이러한 경우 클라이언트는 이전에 연결된 VLAN에서 IP를 계속 요청할 수 있습니다. 이 IP는 현재 VLAN의 DHCP 범위 내에 있지 않으므로 DHCP 서버가 NAK(negative acknowledgement)를 발행하므로 클라이언트가 IP 주소를 획득할 수 없습니다.

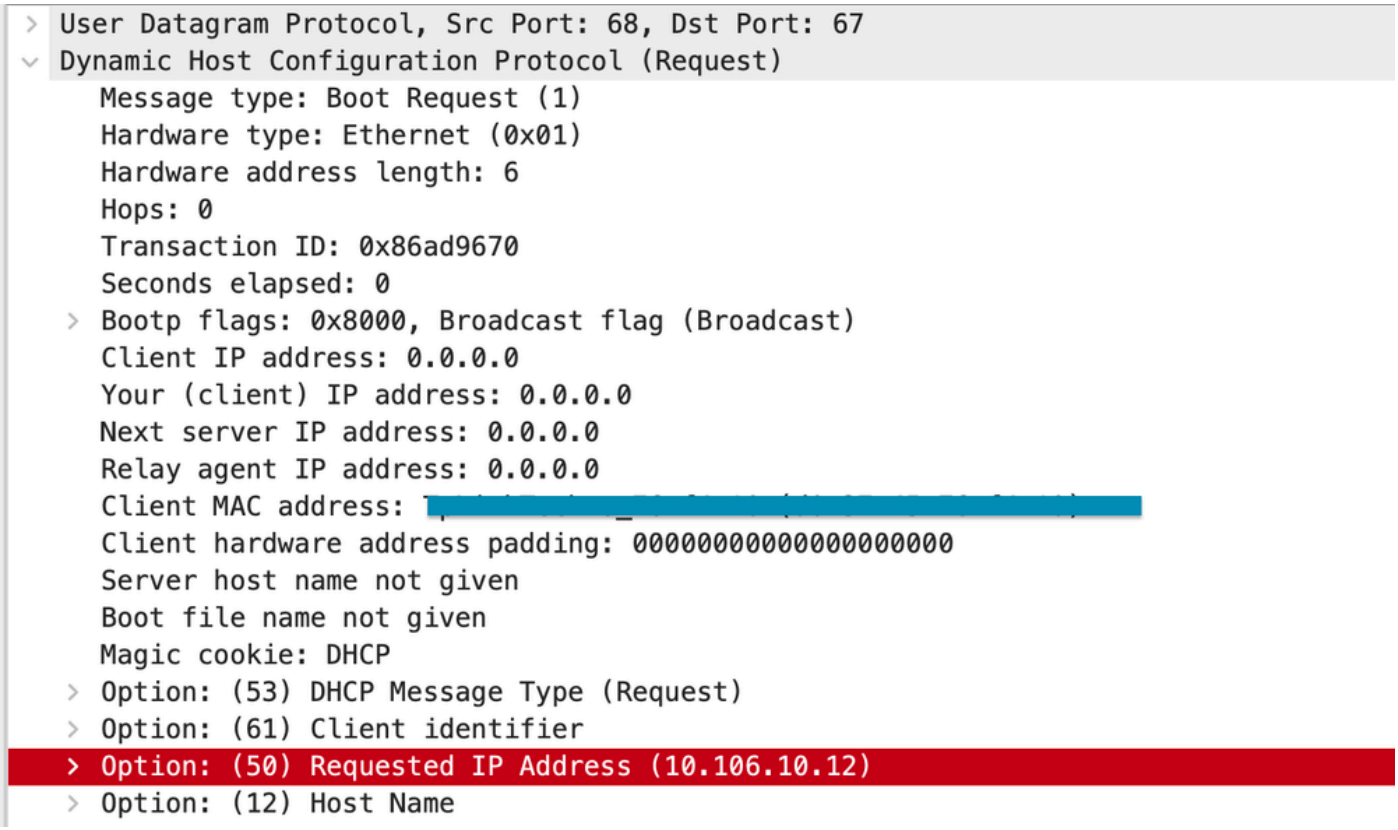
방사성 추적 로그에서 현재 SSID의 클라이언트 VLAN이 VLAN 20임에도 불구하고 클라이언트는 이전에 연결된 VLAN, 즉 VLAN 10에서 IP를 계속 찾습니다.

```
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
```

WLC의 임베디드 패킷 캡처:

```
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
```

WLC의 임베디드 패킷 캡처



WLC 패킷 캡처의 DHCP 옵션 50

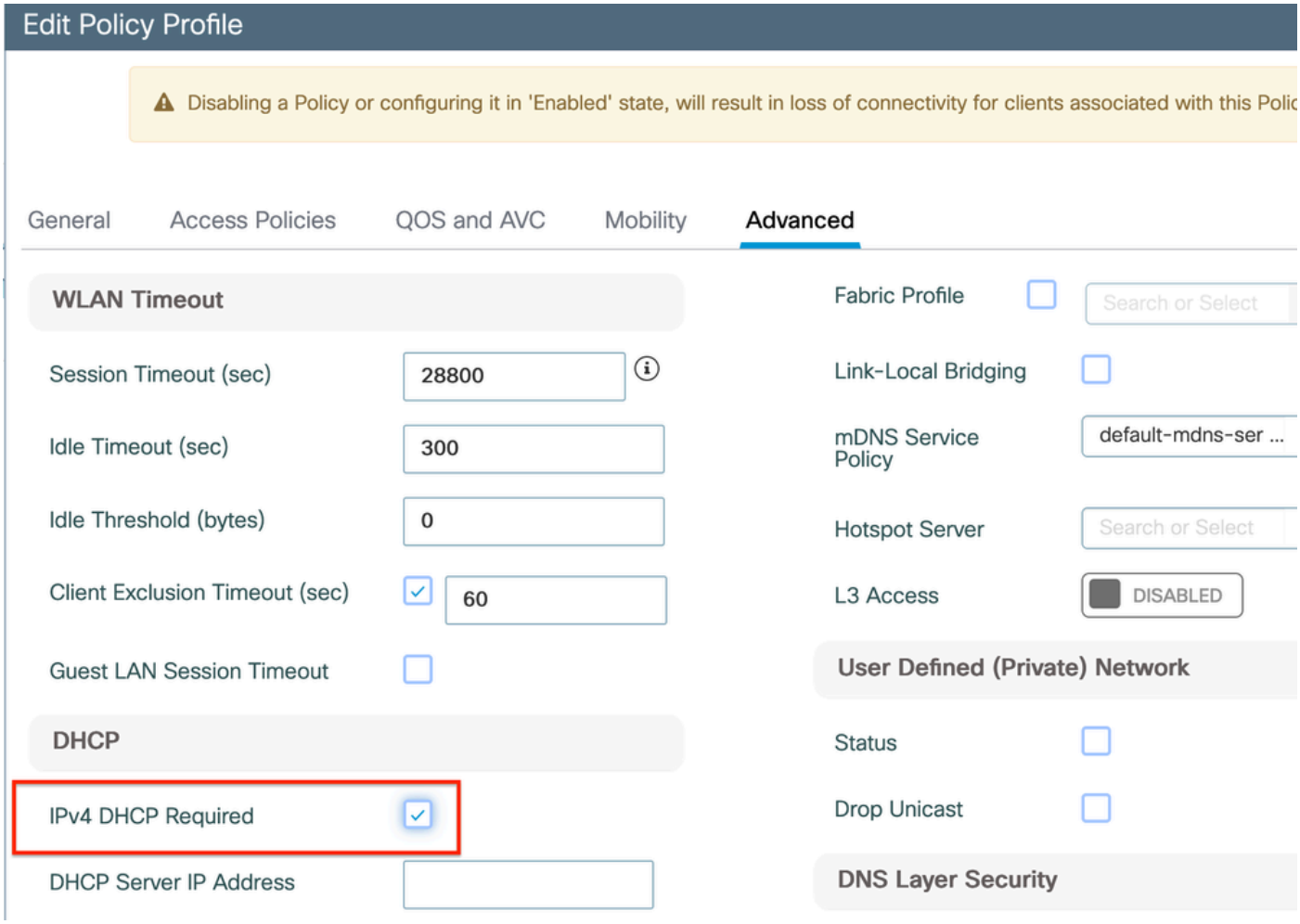
해결 방법: 클라이언트가 전체 DHCP 프로세스를 완료하도록 하려면 정책 컨피그레이션 내에서 IPv4 DHCP Required 옵션을 활성화할 수 있습니다. DHCP 서버가 이전 SSID와 연결된 VLAN에서 IP 주소를 요청할 경우 DHCP 서버가 클라이언트에 NAK를 보낼 수 있도록 하려면 특히 클라이언트가 SSID를 전환할 때 이 설정을 활성화해야 합니다. 그렇지 않으면 클라이언트가 이전에 보유했던 IP 주소를 계속 사용하거나 요청하여 통신이 중단될 수 있습니다. 그러나 이 기능을 활성화하면 고정 IP 주소로 구성된 무선 클라이언트에 영향을 줍니다.

원하는 옵션을 활성화하는 프로세스는 다음과 같습니다.

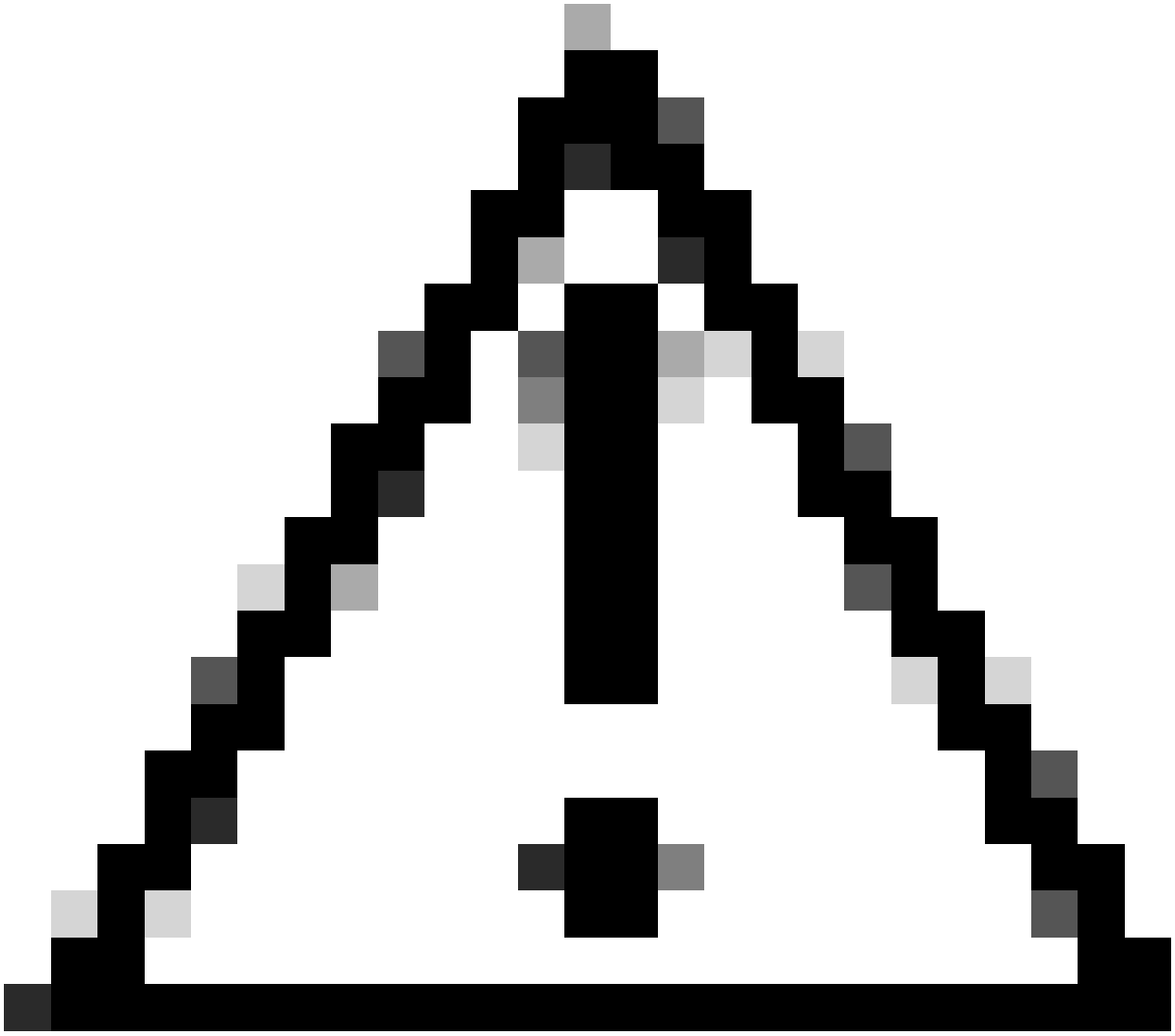
CLI를 통해:

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

Via GUI(GUI 사용): DHCP(Configuration > Tags & Profile > Policy > Policy_name > Advanced. DHCP) 섹션 아래에서 Enable ipv4 DHCP required(ipv4 DHCP 필요)로 이동합니다.



*WLC*의 정책 프로파일 설정



주의: 외부 앵커 설정의 경우, 두 WLC에서 DHCP 설정을 정렬하는 것이 중요합니다. 필수 IPV4 DHCP를 활성화한 경우 외부 및 앵커 WLC 모두에서 활성화해야 합니다. 둘 사이의 정책 프로필 아래에 있는 DHCP 관련 컨피그레이션이 일치하지 않으면 클라이언트에서 모빌리티 역할에 문제가 발생할 수 있습니다.

문제 2: IP 도용 문제로 인해 클라이언트가 삭제되거나 제외되었습니다. IP 도용은 네트워킹 상황에서 둘 이상의 무선 클라이언트가 동일한 IP 주소를 사용하려고 시도하는 상황을 말합니다. 다음과 같은 여러 가지 이유로 인해 발생할 수 있습니다.

1. 무단 고정 IP 할당: 사용자가 장치에서 네트워크에 이미 할당되었거나 지정된 IP와 일치하는 고정 IP 주소를 설정하면 IP 충돌이 발생할 수 있습니다. 이는 두 디바이스가 동일한 IP 주소로 작동하려고 할 때 발생하며, 이 경우 관련 디바이스 중 하나 또는 둘 다의 네트워크 연결이 중단될 수 있습니다. 이러한 문제를 방지하려면 네트워크의 각 클라이언트가 고유한 IP 주소로 구성되어야 합니다.

2. 비인가 DHCP 서버: 네트워크에 비인가 또는 비인가 DHCP 서버가 있으면 IP 주소 할당이 네트워크의 설정된 IP 주소 지정 계획과 충돌할 수 있습니다. 이러한 충돌로 인해 여러 디바이스에서 IP 주소 충돌이 발생하거나 잘못된 네트워크 설정을 가져올 수 있습니다. 이 문제를 해결하려면 네트워크에서 비인가 DHCP 서버를 식별하고 제거하여 동일한 서브넷 내에서 추가 IP 충돌을 방지해야 합니

다.

3. 9800 WLC에서 클라이언트의 오래된 항목: 때때로 컨트롤러는 클라이언트가 획득하려는 IP 주소의 오래된/오래된 항목을 유지할 수 있습니다. 이러한 경우 9800 WLC에서 오래된 항목을 수동으로 제거해야 합니다. 그 방법은 다음과 같습니다.

- 제외 목록에 있는 mac 주소에 대한 방사성 추적을 실행하고 방사성 추적에서 legit mac으로 필터링합니다.
- 오류 로그를 볼 수 있습니다. %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: 클라이언트 MAC: Affected_Client_MAC(IP: 10.37.57.24가 제외 목록에 추가됨), legit 클라이언트 MAC: Legit_Client_MAC, IP: 10.37.57.24, 이유: IP 주소 도난
- 그런 다음 다음 다음 명령을 실행합니다.
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(오래된 항목이 있는 경우 올바른 클라이언트 Mac 주소에 대해 둘 이상의 IP를 볼 수 있습니다. 하나는 원래 IP이고 다른 하나는 오래된/오래된 IP입니다.)

해결 방법: 을 사용하여 9800 WLC에서 오래된 항목을 수동으로 삭제하십시오. clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. 동일한 서브넷을 사용하는 로컬 DHCP 서버를 사용하는 flex 구축: FlexConnect 구성에서는 여러 원격 위치에서 동일한 서브넷의 IP 주소를 할당하는 로컬 DHCP 서버를 사용하는 것이 일반적입니다. 이 시나리오는 다른 사이트의 무선 클라이언트가 동일한 IP 주소를 수신하는 원인이 될 수 있습니다. 이 네트워크 프레임워크 내의 컨트롤러는 여러 클라이언트 연결에서 동일한 IP 주소를 사용하는 경우를 탐지하도록 프로그래밍되어 이를 잠재적인 IP 도용으로 해석합니다. 따라서 이러한 클라이언트는 IP 주소 충돌을 방지하기 위해 대개 차단 목록에 배치됩니다.

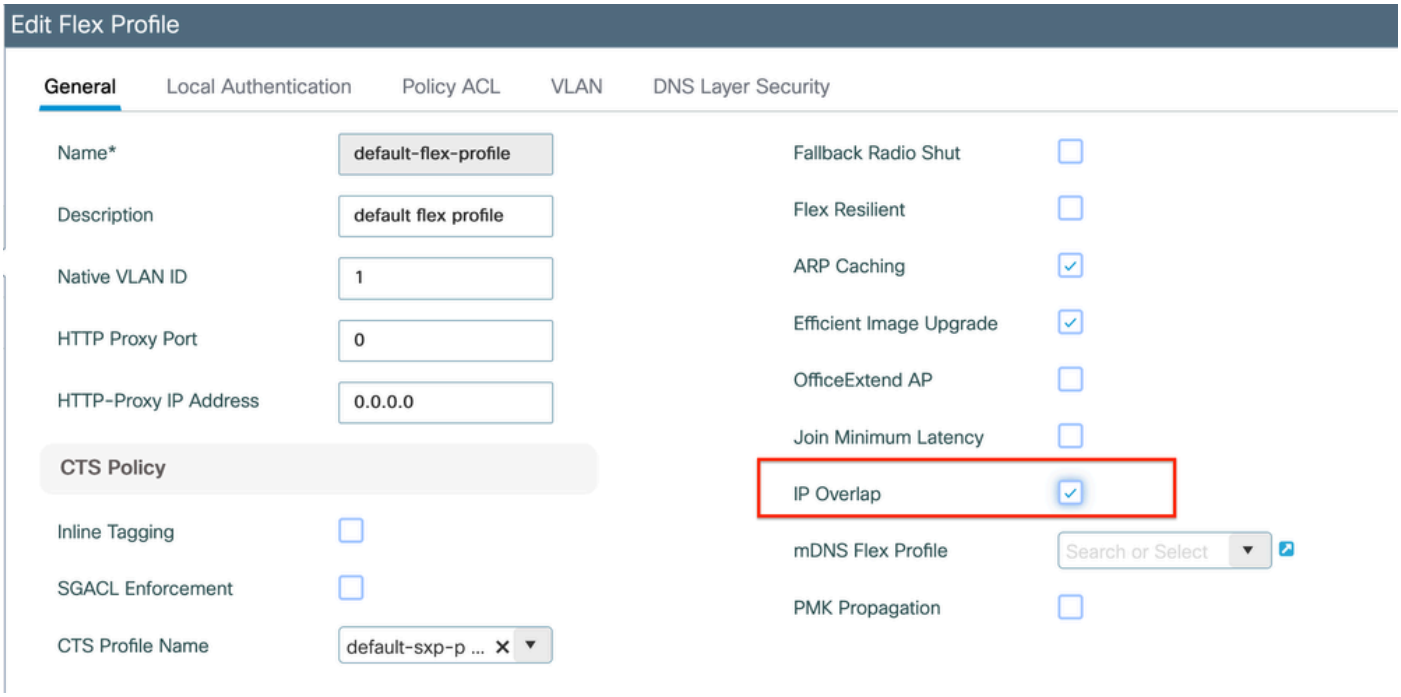
해결 방법: FlexConnect 프로파일 내에서 IP 중복 기능을 활성화합니다. 'Flex 구축의 클라이언트 IP 주소 중복' 기능을 사용하면 FlexConnect 구축에서 지원되는 모든 기능을 유지하면서 여러 FlexConnect 사이트 전체에서 동일한 IP 주소를 사용할 수 있습니다.

기본적으로 이 기능은 비활성화되어 있습니다. 다음 절차에 따라 활성화할 수 있습니다.

CLI를 통해:

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

Via GUI(GUI 사용): Click Existing Flex Profile/Add to new Flex profile(기존 Flex 프로필/새 Flex 프로필에 추가)을 Configuration > Tags & Profiles > Flex. 선택하고 General(일반) 탭에서 IP Overlap(IP 중복)을 활성화합니다.



WLC의 Flex Profile 설정

3호 무선 클라이언트가 의도한 VLAN에서 IP 주소를 수신하지 못하고 있습니다. 이 문제는 VLAN 1을 활용하거나 클라이언트에 할당된 VLAN이 FlexConnect 구축에서 AP 관리에 사용되는 VLAN과 동일할 때 자주 발생합니다. 이 문제의 근본 원인은 일반적으로 잘못된 VLAN 할당입니다. 지침을 제공하기 위해 9800 Series에서 VLAN ID를 구성할 때 고려해야 할 몇 가지 시나리오가 있습니다.

1. AAA 재정의 기능이 활성화된 AAA 서버를 사용할 경우, AAA 서버에서 적절한 VLAN ID를 전송해야 합니다. VLAN 이름이 대신 제공되는 경우 9800 WLC에 구성된 VLAN 이름과 일치하는지 확인합니다.

2. VLAN 1이 무선 클라이언트 트래픽에 대해 구성된 경우 동작은 액세스 포인트(AP)의 모드에 따라 달라질 수 있습니다.

로컬 모드/중앙 스위칭의 AP:

- VLAN-name = 기본값을 지정하면 클라이언트는 VLAN 1에 할당됩니다.
- VLAN-ID 1을 사용하여 무선 관리 VLAN에 클라이언트가 할당됩니다

Flex 모드/로컬 스위칭의 AP:

- VLAN-name = 기본값을 지정하면 클라이언트는 VLAN 1에 할당됩니다.
- VLAN-ID 1을 사용하면 클라이언트가 FlexConnect 네이티브 VLAN에 할당됩니다

이 실습에서 실험한 시나리오의 몇 가지 예는 그 결과와 함께 다음과 같습니다.

1. 기본적으로 사용자가 정책 프로필에서 아무 것도 구성하지 않으면 WLC에서 VLAN-ID 1을 할당하므로 클라이언트는 로컬 모드에서 무선 관리 VLAN을 사용하고 FlexConnect에 AP 기본 VLAN을 사용합니다.

2. flex-profile 아래의 Native-VLAN이 스위치에 구성된 것과 다른 Native VLAN ID로 구성된 경우, 문제가 나타나며, 정책 프로파일이 "기본" VLAN 이름으로 구성된 경우에도 클라이언트는 관리 VLAN(Native VLAN)에서 IP를 가져옵니다.

3. flex-profile 아래의 Native-VLAN이 스위치에 구성된 네이티브 VLAN과 동일한 VLAN-ID로 구성된 경우 클라이언트만 정책 프로필에 구성된 기본값으로 VLAN 1에서 IP를 가져올 수 있습니다.

4. VLAN ID 대신 VLAN 이름을 선택한 경우 Flex 프로파일의 VLAN 이름이 동일한지 확인합니다.

관련 정보

- 9800의 내부 DHCP 서버
- 외부 DHCP 서버가 사용 중입니다.
- Windows DHCP 서버의 DHCP 옵션 82 하위 옵션 5
- Flex AP의 NAT-PAT
- VLAN 1은 무선 클라이언트에 사용됩니다
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.