AireOS WLC가 DHCP 프로토콜을 처리하는 방식 이해

목차

소개

이 문서에서는 Cisco AireOS 무선 컨트롤러의 다양한 DHCP 작업에 대해 설명합니다.

외부 DHCP 서버

WLC(Wireless LAN Controller)는 외부 DHCP 서버를 사용하는 경우 두 가지 DHCP 작업 모드를 지원합니다.

- DHCP 프록시 모드
- DHCP 브리징 모드

DHCP 프록시 모드는 DHCP 서버와 무선 클라이언트 간의 DHCP 트랜잭션에 대한 보안 및 제어를 향상하기 위해 DHCP 헬퍼 기능 역할을 합니다. DHCP 브리징 모드는 DHCP 트랜잭션에서 컨트롤러 역할을 무선 클라이언트에 투명하게 만드는 옵션을 제공합니다.

DHCP 프록시 및 브리징 모드 비교

클라이언트 DHCP 처리	DHCP 프록시 모드	DHCP 브리징 모드
giaddr 수정	예	아니요
siaddr 수정	예	아니요
패킷 내용 수정	예	아니요
이중화 오퍼가 전달되지 않음	예	아니요
옵션 82 지원	예	아니요
유니캐스트에 브로드캐스트	예	아니요
BOOTP 지원	아니요	서버
RFC 비규격	프록시와 릴레이 에이전트는 정확히 동일한 개념이 아닙니다. DHCP 브리징 모드는 전체 RFC 규정 준수를 위해 권장됩니다.	아니요

DHCP 프록시 모드

DHCP 프록시는 모든 네트워크 환경에 적합하지 않습니다. 컨트롤러는 도우미 기능을 제공하고 특정 보안 문제를 해결하기 위해 모든 DHCP 트랜잭션을 수정 및 릴레이합니다.

컨트롤러 가상 IP 주소는 일반적으로 클라이언트에 대한 모든 DHCP 트랜잭션의 소스 IP 주소로 사용됩니다. 따라서 실제 DHCP 서버 IP 주소가 외부에 노출되지 않습니다. 이 가상 IP는 컨트롤러의 DHCP 트랜잭션에 대한 디버그 출력에 표시됩니다. 그러나 가상 IP 주소를 사용하면 특정 유형의 클라이언트에 문제가 발생할 수 있습니다.

DHCP 프록시 모드 작업은 대칭 및 비대칭 모빌리티 프로토콜 모두에 대해 동일한 동작을 유지합니다.

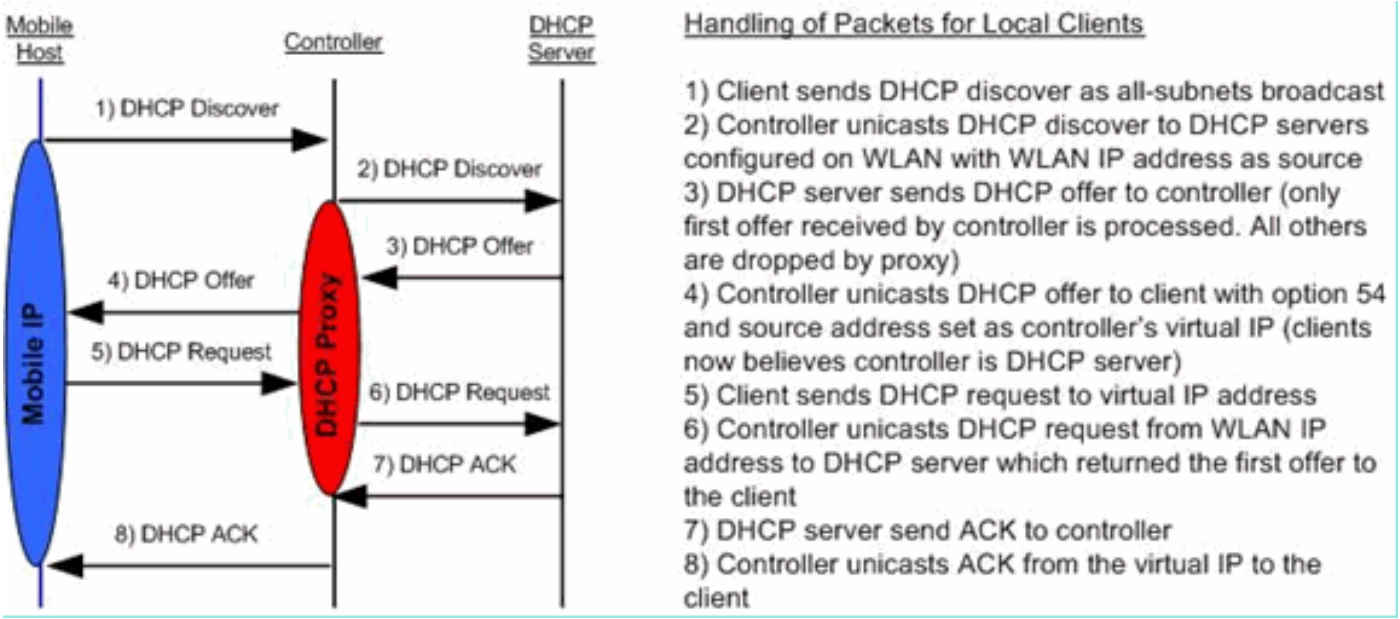
외부 DHCP 서버에서 여러 오퍼가 오는 경우 DHCP 프록시는 일반적으로 들어오는 첫 번째 오퍼를 선택하고 클라이언트 데이터 구조에서 서버의 IP 주소를 설정합니다. 따라서 모든 후속 트랜잭션은

재시도 후 트랜잭션이 실패할 때까지 동일한 DHCP 서버를 통해 실행됩니다. 이때 프록시는 클라이언트에 대해 다른 DHCP 서버를 선택합니다.

DHCP 프록시는 기본적으로 활성화되어 있습니다. 통신하는 모든 컨트롤러의 DHCP 프록시 설정이 동일해야 합니다.

참고: DHCP 옵션 82가 올바르게 작동하려면 DHCP 프록시를 활성화해야 합니다.

프록시 패킷 흐름

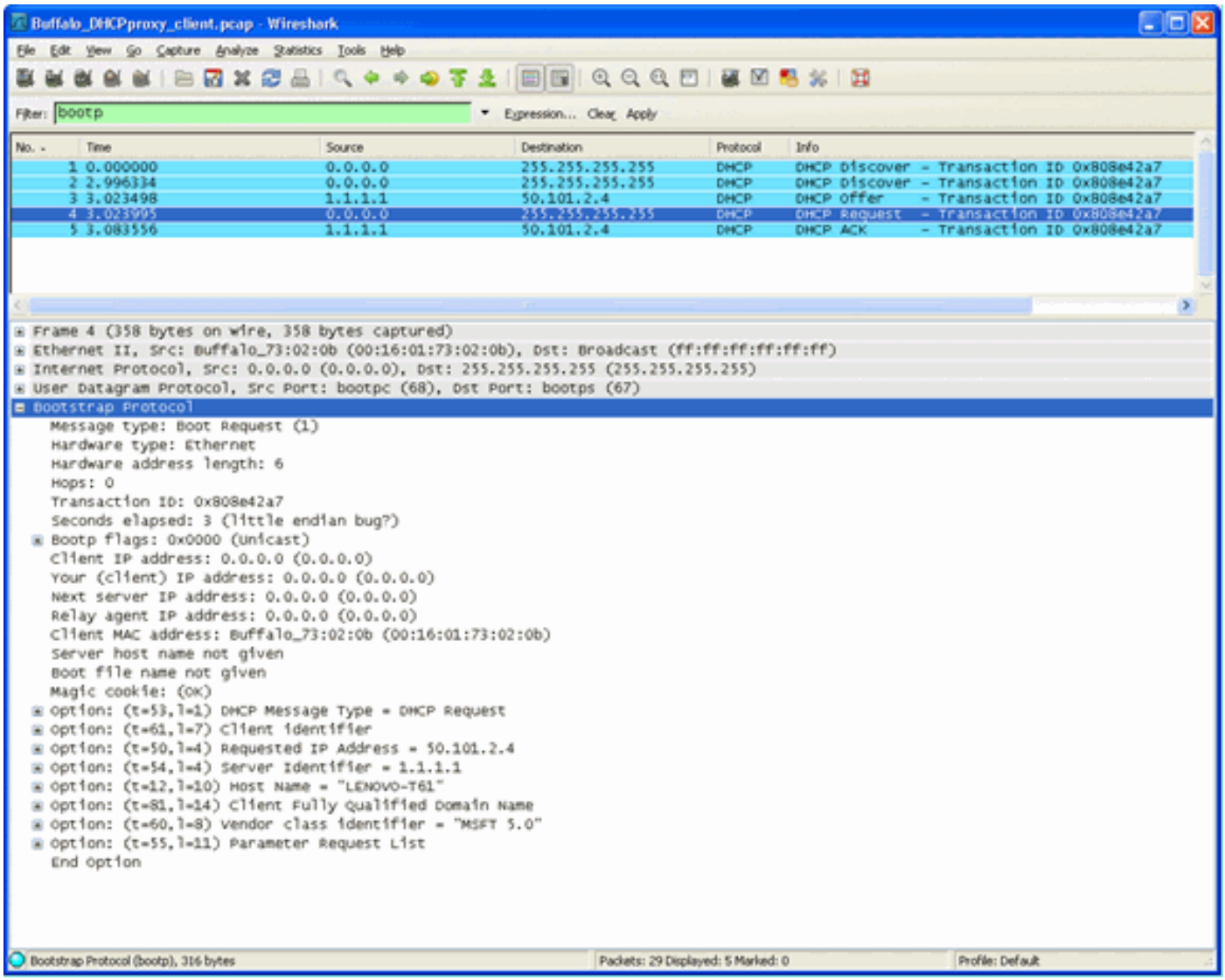


프록시 패킷 캡처

컨트롤러가 DHCP 프록시 모드에 있을 때 DHCP 패킷을 DHCP 서버로 전달할 뿐만 아니라 실제로 DHCP 서버로 전달할 새 DHCP 패킷을 작성합니다. 클라이언트 DHCP 패킷에 있는 모든 DHCP 옵션은 컨트롤러 DHCP 패킷에 복사됩니다. 다음 스크린샷 예에서는 DHCP 요청 패킷에 대해 이를 보여줍니다.

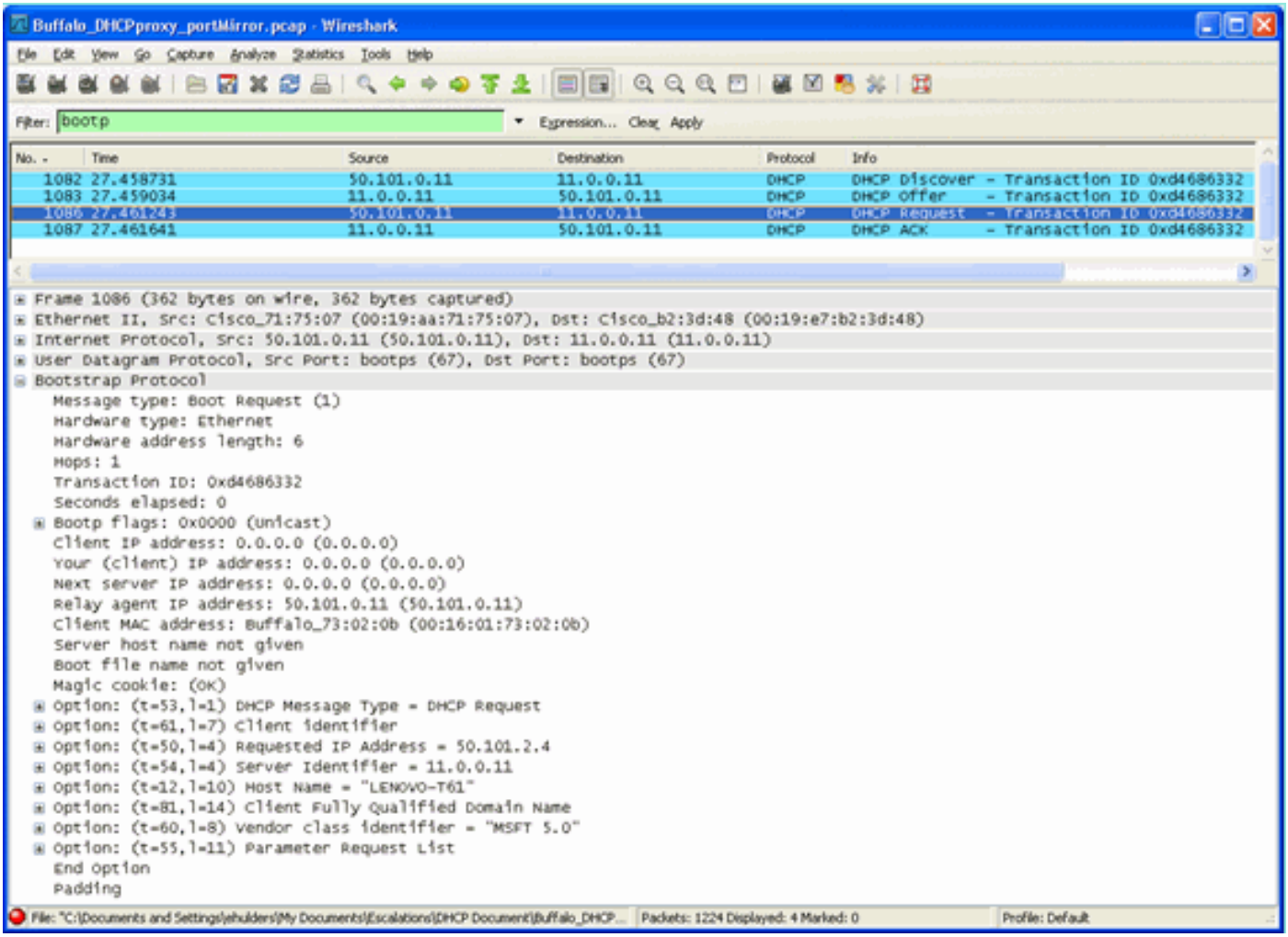
클라이언트 관점

이 스크린샷은 클라이언트의 관점에서 찍은 패킷 캡처입니다. DHCP 검색, DHCP 오퍼, DHCP 요청 및 DHCP ACK가 표시됩니다. DHCP 요청이 강조 표시되고 bootp protocol detail이 확장되어 DHCP 옵션이 표시됩니다.



서버 관점

이 스크린샷은 서버의 관점에서 찍은 패킷 캡처입니다. 앞의 예와 마찬가지로 DHCP discover, DHCP offer, DHCP request 및 DHCP ACK를 보여 줍니다. 그러나 이는 컨트롤러가 DHCP 프록시의 기능으로 구축한 패킷입니다. 다시 DHCP 요청이 강조 표시되고 boot p protocol detail이 확장되어 DHCP 옵션이 표시됩니다. 클라이언트의 DHCP 요청 패킷과 동일합니다. 또한 WLC 프록시가 패킷을 릴레이하고 패킷 주소를 강조 표시합니다.



프록시 컨피그레이션 예

컨트롤러를 DHCP 프록시로 사용하려면 컨트롤러에서 DHCP 프록시 기능을 활성화해야 합니다. 기본적으로 이 기능은 활성화되어 있습니다. DHCP 프록시를 활성화하기 위해 이 CLI 명령을 사용할 수 있습니다. DHCP 메뉴의 Controller(컨트롤러) 페이지에 있는 GUI에서도 동일한 기능을 사용할 수 있습니다.

<#root>

```
(Cisco Controller) >
```

config dhcp proxy enable

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behavior: enabled
```

DHCP 프록시가 작동하려면 DHCP 서비스가 필요한 각 컨트롤러 인터페이스에 기본 DHCP 서버를 구성해야 합니다. DHCP 서버는 관리 인터페이스, ap-manager 인터페이스 및 동적 인터페이스에서 구성할 수 있습니다. 각 인터페이스에 대해 DHCP 서버를 구성하기 위해 이러한 CLI 명령을 사용할

수 있습니다.

```
<#root>
(Cisco Controller) >
config interface dhcp ap-manager primary

(Cisco Controller) >
config interface dhcp management primary

(Cisco Controller) >
config interface dhcp dynamic-interface

 primary
```

DHCP 브리징 기능은 전역 설정이므로 컨트롤러 내의 모든 DHCP 트랜잭션에 영향을 줍니다.

문제 해결

이는 Cisco의 **debug dhcp packet enable** 명령을 실행합니다. 디버그는 MAC 주소가 00:40:96:b4:8c:e1인 클라이언트로부터 DHCP 요청을 수신하고 DHCP 서버에 DHCP 요청을 전송하고 DHCP 서버로부터 응답을 수신하고 클라이언트에 DHCP 제공을 전송하는 컨트롤러를 보여줍니다.

```
<#root>
(Cisco Controller) >
debug dhcp message enable

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP received op BOOTREQUEST (1)
```

(len 312, port 29, encap 0xec03)

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len (including the magic cookie) 76
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message type = DHCP REQUEST
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 61 (len 7) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: requested ip = 192.168.4.13
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 12 (len 7) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 81 (len 11) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: vendor class id = MSFT 5.0 (len 8)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 55 (len 11) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP options end, len 76, actual 68
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
```

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selected relay 1 - 192.168.3.1 (local address 192.168.4.2, gateway 192.168.4.1, VLAN 101, port 29)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP transmitting DHCP REQUEST (3)

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   op: BOOTREQUEST, htype: Ethernet,
 hlen: 6, hops: 1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   xid: 0xfc3c9979 (4231829881), secs: 0,
 flags: 0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   chaddr: 00:40:96:b4:8c:e1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   siaddr: 0.0.0.0,  giaddr: 192.168.4.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   requested ip: 192.168.4.13
```

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP Forwarding DHCP packet (332 octets)
-- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 192.168.4.1

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REQUEST to 192.168.4.1
 (len 350, port 29, vlan 101)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 192.168.4.1  VLAN: 101
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selected relay 2 - NONE
```

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP received op BOOTREPLY (2) (len 316, port 29, encap 0xec00)

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len (including the magic cookie) 80
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message type = DHCP ACK
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 58 (len 4) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 59 (len 4) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: lease time = 691200 seconds
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: server id = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: netmask = 255.255.0.0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 15 (len 14) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: gateway = 192.168.4.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: DNS server, cnt = 1, first = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: WINS server, cnt = 1, first = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP options end, len 80, actual 72
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP setting server from ACK (server 192.168.3.1,
 yiaddr 192.168.4.13)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 Assigning Address 192.168.4.13 to mobile
```

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REPLY to STA (len 424, port 29, vlan 20)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP transmitting DHCP ACK (5)

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6,
 hops: 0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   xid: 0xfc3c9979 (4231829881), secs: 0,
```

```
 flags: 0
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   chaddr: 00:40:96:b4:8c:e1
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   ciaddr: 0.0.0.0,  yiaddr: 192.168.4.13
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   server id: 192.0.2.10  rcvd server id: 192.168.3.1
```

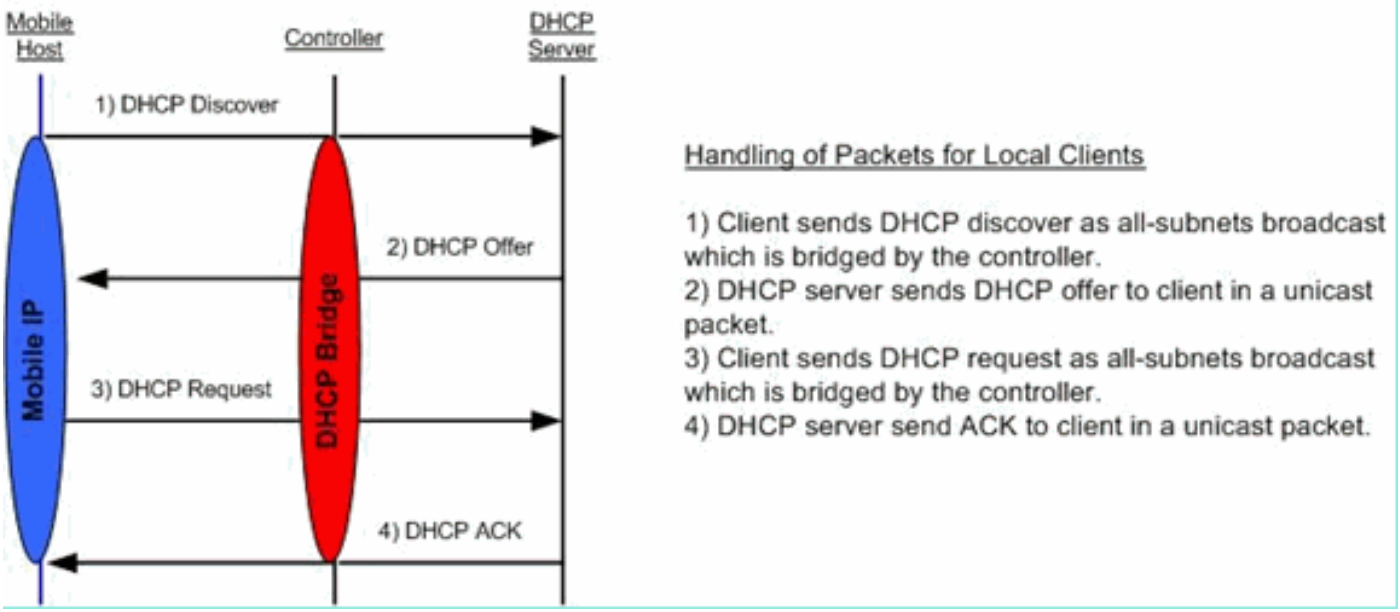
경고

- DHCP 프록시가 활성화된 컨트롤러와 방화벽 및 DHCP 서버 역할을 하는 디바이스 간에는 상호 운용성 문제가 있을 수 있습니다. 이는 일반적으로 방화벽이 프록시 요청에 응답하지 않기 때문에 디바이스의 방화벽 구성 요소 때문일 가능성이 높습니다. 이 문제의 해결 방법은 컨트롤러에서 DHCP 프록시를 비활성화하는 것입니다.
- 클라이언트가 컨트롤러에서 DHCP REQ 상태에 있으면 컨트롤러는 DHCP 알림 패킷을 삭제합니다. 클라이언트에서 DHCP 검색 패킷을 수신할 때까지 클라이언트는 컨트롤러에서 RUN 상태로 전환되지 않습니다(클라이언트가 트래픽을 전달하는 데 필요함). DHCP 알림 패킷은 DHCP 프록시가 비활성화된 경우 컨트롤러에 의해 전달됩니다.
- 서로 통신하는 모든 컨트롤러에는 동일한 DHCP 프록시 설정이 있어야 합니다.

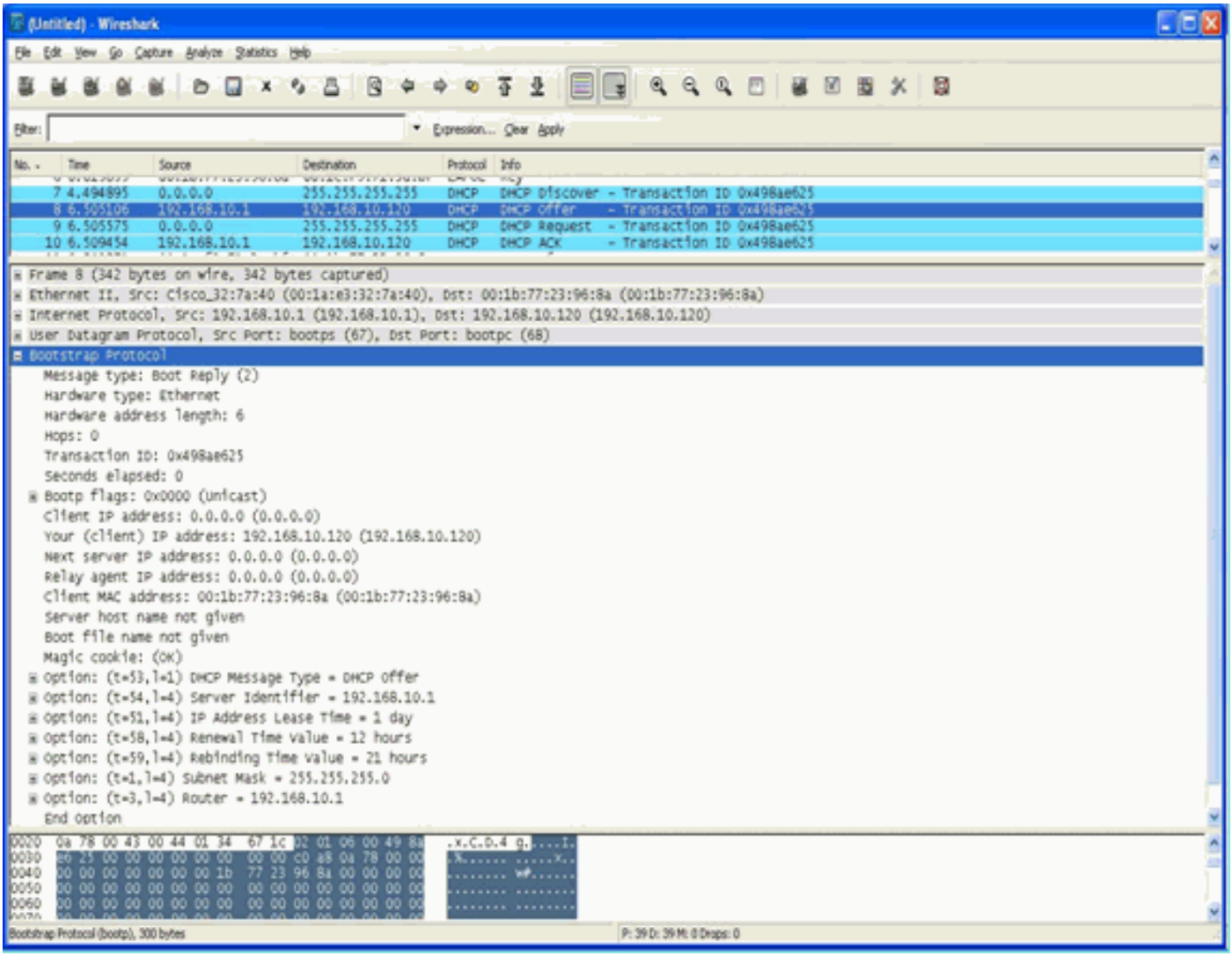
DHCP 브리징 모드

DHCP 브리징 기능은 DHCP 트랜잭션에서 컨트롤러 역할을 클라이언트에 투명하게 만들도록 설계되었습니다. 802.11에서 이더넷 II로 변환하는 경우를 제외하고, 클라이언트의 패킷은 LWAPP(Light Weight Access Point Protocol) 터널에서 수정되지 않은 상태로 클라이언트 VLAN(또는 L3 로밍 사례의 EoIP(Ethernet over IP) 터널)에 연결됩니다. 마찬가지로, 이더넷 II를 802.11로 변환하는 경우를 제외하고 클라이언트로 보내는 패킷은 클라이언트 VLAN(또는 L3 로밍 사례의 EoIP 터널)에서 LWAPP 터널로 수정되지 않은 브리지로 연결됩니다. 이를 스위치 포트에 클라이언트를 연결한 다음 기존 DHCP 트랜잭션을 수행하는 것으로 간주합니다.

DHCP 브리징 작업 - 브리징 패킷 흐름

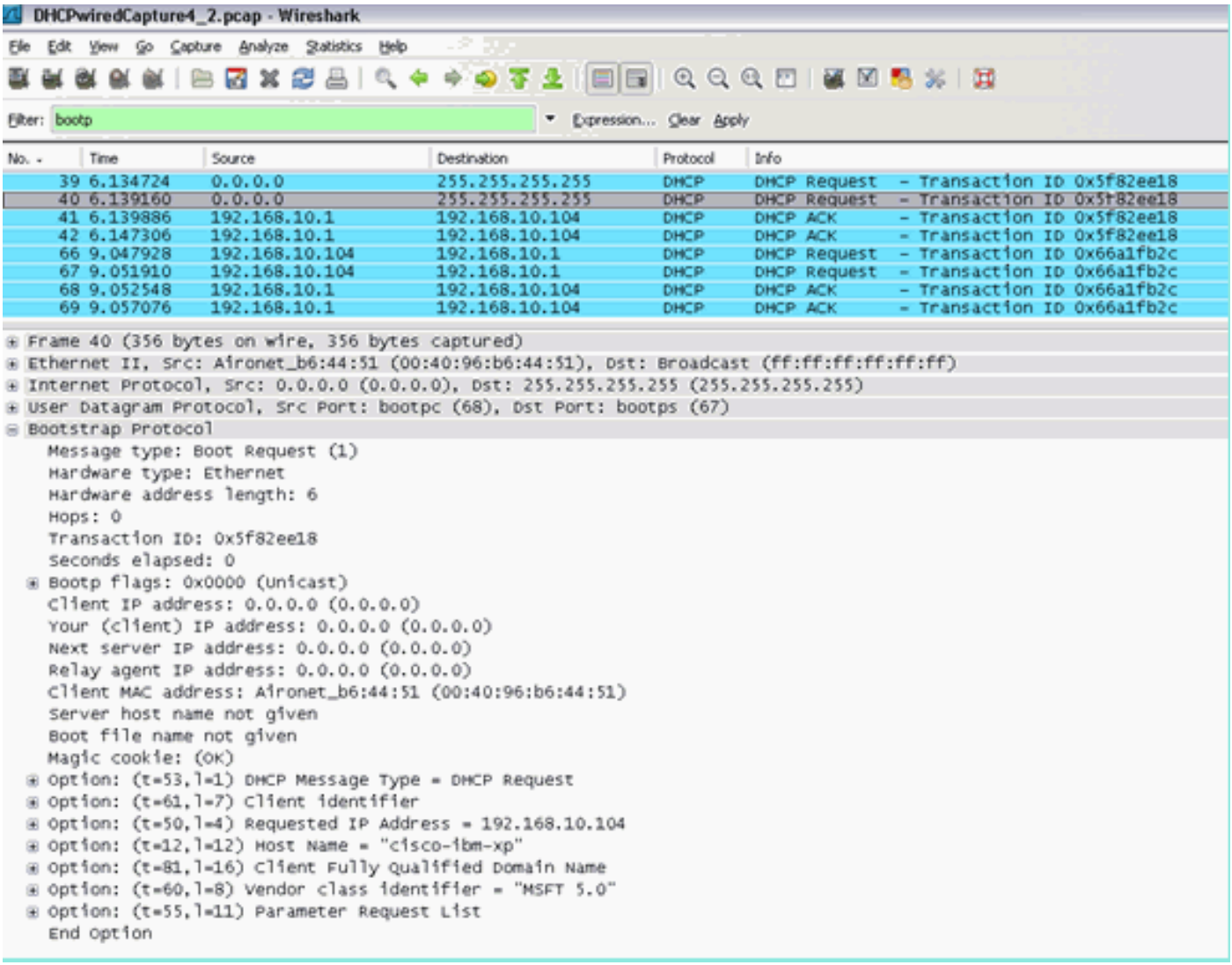


브리징 패킷 캡처 - 클라이언트 관점



클라이언트 측 패킷 캡처 스크린샷에서 프록시 모드의 클라이언트 캡처 간 주요 차이점은 DHCP 서버의 실제 IP입니다. 이 IP는 컨트롤러 가상 IP 주소 대신 Offer 및 Ack 패킷에 표시됩니다.

브리징 패킷 캡처 - 서버 관점



유선 패킷 캡처 스크린샷에서는 패킷 40이 테스트 클라이언트에서 유선 네트워크로 연결된 DHCP 요청 브로드캐스트(00:40:96:b6:44:51)임을 확인할 수 있습니다.

브리징 컨피그레이션 예

컨트롤러에서 DHCP 브리징 기능을 활성화하려면 컨트롤러에서 DHCP 프록시 기능을 비활성화해야 합니다. 이 작업은 CLI에서 다음 명령을 사용해야만 수행할 수 있습니다.

```
<#root>

(Cisco Controller) >

config dhcp proxy disable

(Cisco Controller) >

show dhcp proxy

DHCP Proxy Behaviour: disabled
```

DHCP 서버가 클라이언트와 동일한 L2(Layer 2) 네트워크에 없는 경우 IP 헬퍼를 사용하여 클라이

언트 게이트웨이에서 DHCP 서버에 브로드캐스트를 전달해야 합니다. 다음은 이 구성의 예입니다.

```
<#root>

Switch#

conf t

Switch(config)#

interface vlan




Switch(config-if)#

ip helper-address
```

DHCP 브리징 기능은 전역 설정이므로 컨트롤러 내의 모든 DHCP 트랜잭션에 영향을 줍니다. 컨트롤러에서 필요한 모든 VLAN에 대해 유선 인프라에서 IP 헬퍼 명령문을 추가해야 합니다.

문제 해결

여기에 나열된 디버그는 컨트롤러 CLI에서 활성화되었으며 이 문서에 대한 출력의 DHCP 부분이 추출되었습니다.

```
<#root>

(Cisco Controller) >

debug client 00:40:96:b6:44:51

(Cisco Controller) >

debug dhcp message enable


00:40:96:b6:44:51 DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 72
00:40:96:b6:44:51 DHCP option: message type = DHCP DISCOVER
00:40:96:b6:44:51 DHCP option: 116 (len 1) - skipping
00:40:96:b6:44:51 DHCP option: 61 (len 7) - skipping
00:40:96:b6:44:51 DHCP option: 12 (len 12) - skipping
00:40:96:b6:44:51 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:40:96:b6:44:51 DHCP option: 55 (len 11) - skipping
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP DISCOVER (1)
00:40:96:b6:44:51 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP   xid: 0x224dfab6 (575535798), secs: 0, flags: 0
```

```
00:40:96:b6:44:51 DHCP   chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
```

00:40:96:b6:44:51 DHCP successfully bridged packet to DS

```
00:40:96:b6:44:51 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 72
00:40:96:b6:44:51 DHCP option: message type = DHCP OFFER
```

00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1

```
00:40:96:b6:44:51 DHCP option: lease time = 84263 seconds
00:40:96:b6:44:51 DHCP option: 58 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: 59 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP option: gateway = 192.168.10.1
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP OFFER (2)
00:40:96:b6:44:51 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP   xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP   chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP   ciaddr: 0.0.0.0,  yiaddr: 192.168.10.104
00:40:96:b6:44:51 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   server id: 192.168.10.1  rcvd server id: 192.168.10.1
```

00:40:96:b6:44:51 DHCP successfully bridged packet to STA

```
00:40:96:b6:44:51 DHCP received op BOOTREQUEST (1) (len 328, port 1, encap 0xec03)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 92
00:40:96:b6:44:51 DHCP option: message type = DHCP REQUEST
00:40:96:b6:44:51 DHCP option: 61 (len 7) - skipping
00:40:96:b6:44:51 DHCP option: requested ip = 192.168.10.104
00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1
00:40:96:b6:44:51 DHCP option: 12 (len 12) - skipping
00:40:96:b6:44:51 DHCP option: 81 (len 16) - skipping
00:40:96:b6:44:51 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:40:96:b6:44:51 DHCP option: 55 (len 11) - skipping
00:40:96:b6:44:51 DHCP options end, len 92, actual 84
00:40:96:b6:44:51 DHCP processing DHCP REQUEST (3)
00:40:96:b6:44:51 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP   xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP   chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   requested ip: 192.168.10.104
00:40:96:b6:44:51 DHCP   server id: 192.168.10.1  rcvd server id: 192.168.10.1
```

00:40:96:b6:44:51 DHCP successfully bridged packet to DS

```
00:40:96:b6:44:51 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
00:40:96:b6:44:51 DHCP option len (including the magic
cookie) 72 00:40:96:b6:44:51 DHCP option: message type = DHCP ACK
00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1
00:40:96:b6:44:51 DHCP option: lease time = 86400 seconds
00:40:96:b6:44:51 DHCP option: 58 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: 59 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP option: gateway = 192.168.10.1
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP ACK (5)
00:40:96:b6:44:51 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP   xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP   chaddr: 00:40:96:b6:44:51
```

```
00:40:96:b6:44:51 DHCP   ciaddr: 0.0.0.0,  yiaddr: 192.168.10.104
00:40:96:b6:44:51 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   server id: 192.168.10.1  rcvd server id: 192.168.10.1

00:40:96:b6:44:51 Assigning Address 192.168.10.104 to mobile
00:40:96:b6:44:51 DHCP successfully bridged packet to STA
00:40:96:b6:44:51 192.168.10.104 Added NPU entry of type 1
```

이 DHCP 디버그 출력에는 컨트롤러에서 DHCP 브리징을 사용 중임을 나타내는 몇 가지 주요 표시가 있습니다.

- DHCP가 성공적으로 패킷을 DS에 브리지함 - 클라이언트에서 원래 DHCP 패킷을 DS(배포 시스템)로 변경하지 않고 브리지했음을 의미합니다. DS는 유선 인프라입니다.
- DHCP가 성공적으로 패킷을 STA에 브리지함 - 이 메시지는 DHCP 패킷이 브리지되었지만 스테이션(STA)에 변경되지 않았음을 나타냅니다. STA는 DHCP를 요청하는 클라이언트 머신입니다.

또한 디버그에 나열된 실제 서버 IP 주소(192.168.10.1)가 표시됩니다. DHCP 브리징 대신 DHCP 프록시를 사용하는 경우 서버 IP 주소에 대해 나열된 컨트롤러 가상 IP 주소를 확인할 수 있습니다.

경고

- 기본적으로 DHCP 프록시는 활성화되어 있습니다.
- 서로 통신하는 모든 컨트롤러에는 동일한 DHCP 프록시 설정이 있어야 합니다.
- DHCP 옵션 82가 작동하려면 DHCP 프록시를 사용하도록 설정해야 합니다.

내부 DHCP 서버

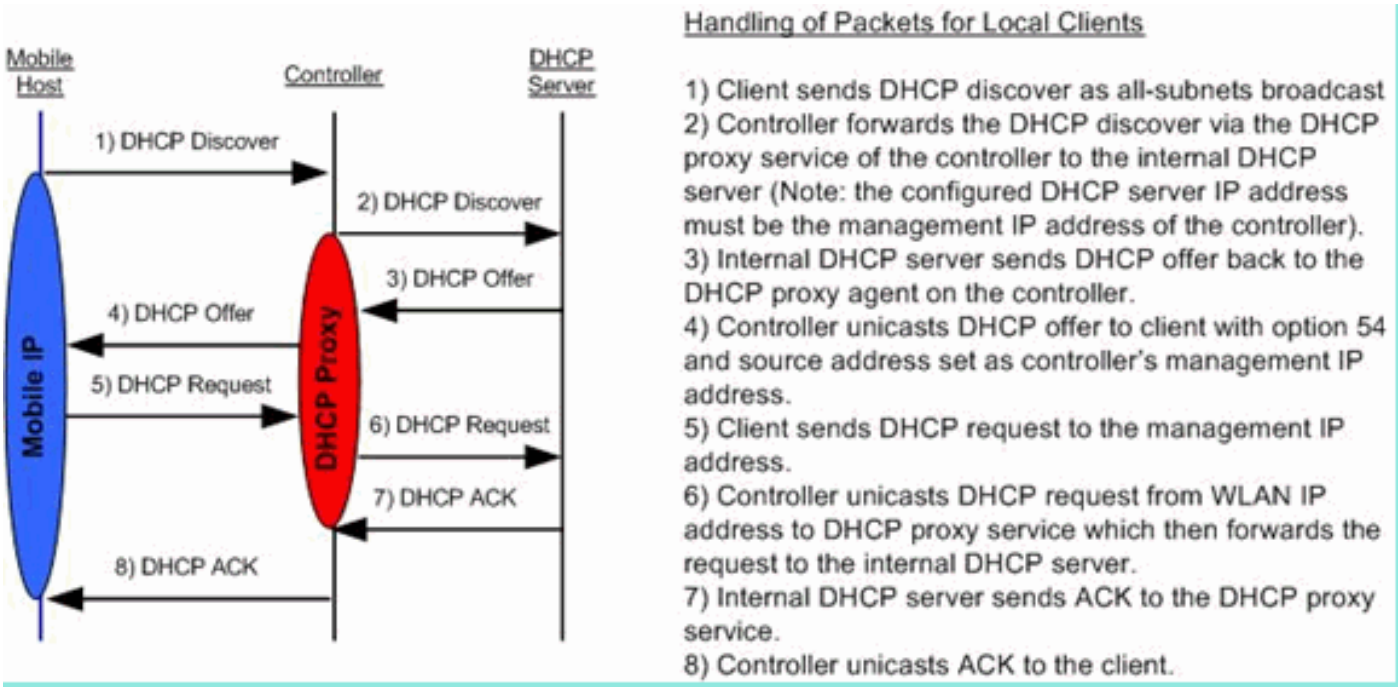
내부 DHCP 서버는 처음에 외부 DHCP 서버를 사용할 수 없는 지사에 도입되었습니다. 동일한 서브넷에 있는 10개 미만의 AP(Access Point)를 사용하는 소규모 무선 네트워크를 지원하도록 설계되었습니다. 내부 서버는 무선 클라이언트, 직접 연결 AP, 관리 인터페이스의 어플라이언스 모드 AP, AP에서 릴레이된 DHCP 요청에 IP 주소를 제공합니다. 이는 완전한 범용 DHCP 서버가 아닙니다. 제한된 기능만 지원하고 대규모 구축에서는 확장하지 않습니다.

내부 DHCP 및 브리징 모드 비교

컨트롤러의 두 가지 기본 DHCP 모드는 DHCP 프록시 또는 DHCP 브리징입니다. DHCP 브리징을 사용하면 컨트롤러가 자동 AP를 사용하는 DHCP처럼 작동합니다. VLAN에 연결된 SSID(Service Set Identifier)에 대한 클라이언트 연결을 통해 DHCP 패킷이 AP로 들어옵니다. 그런 다음 DHCP 패킷이 해당 VLAN에서 나갑니다. 해당 VLAN의 L3(Layer 3) 게이트웨이에 IP 헬퍼가 정의되어 있는 경우 패킷은 직접 유니캐스트를 통해 해당 DHCP 서버에 전달됩니다. 그런 다음 DHCP 서버는 해당 DHCP 패킷을 전달한 L3 인터페이스에 직접 응답합니다. DHCP 프록시의 경우에도 마찬가지이지만, 모든 전달은 VLAN의 L3 인터페이스가 아닌 컨트롤러에서 직접 이루어집니다. 예를 들어 클라이언트에서 WLAN에 DHCP 요청을 보내면 WLAN은 VLAN의 인터페이스에 정의된 DHCP 서버를 사용하거나 *또는*는 VLAN 인터페이스의 IP 주소로 채워지는 DHCP 패킷 GIADDR 필드를 사용하여 유니캐스트 DHCP 패킷을 DHCP 서버에 전달하기 위해 WLAN의 DHCP 재정의 기능을 사용합

니다.

내부 DHCP 서버 - 패킷 흐름

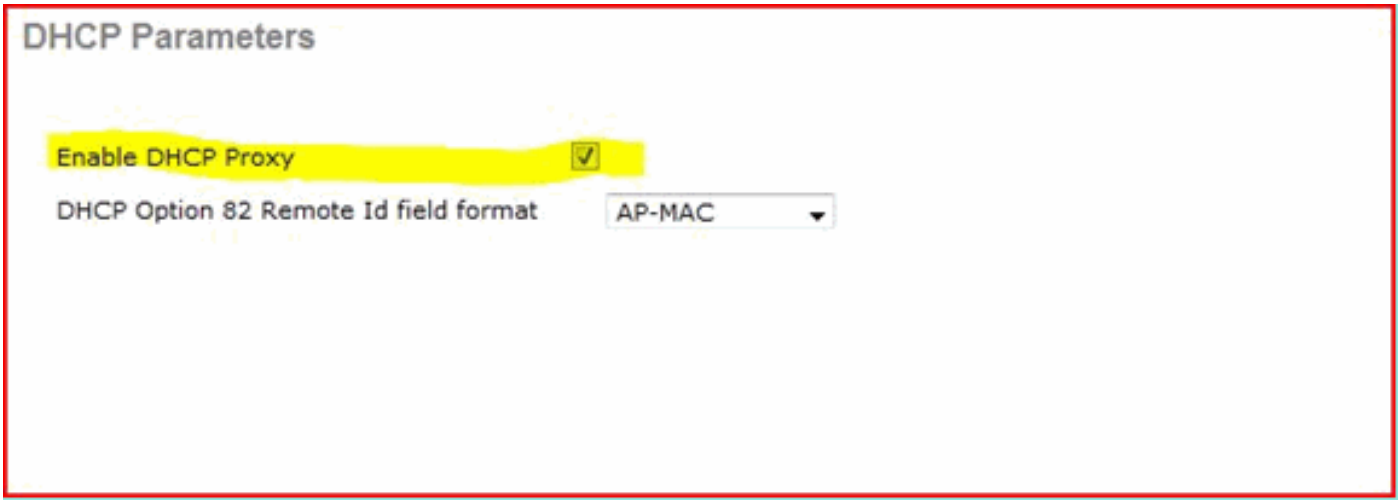


내부 DHCP 서버 컨피그레이션 예

내부 DHCP 서버가 작동하도록 하려면 컨트롤러에서 DHCP 프록시를 활성화해야 합니다. 이 섹션의 GUI를 통해 수행할 수 있습니다.

참고: 모든 버전에서 GUI를 통해 DHCP 프록시를 설정할 수는 없습니다.

```
Controller->Advanced->DHCP
```

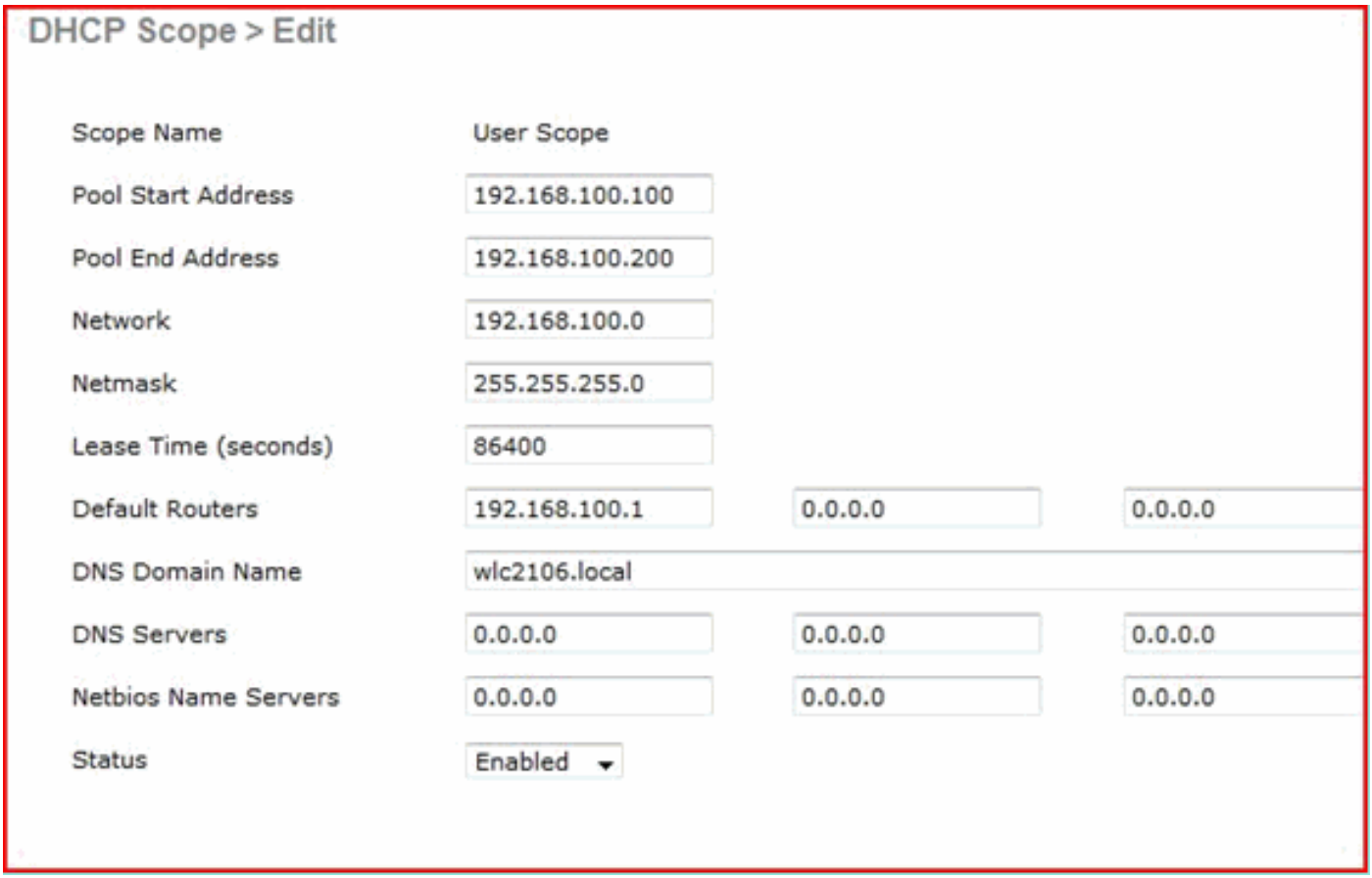


또는 CLI를 통해 다음을 수행합니다.

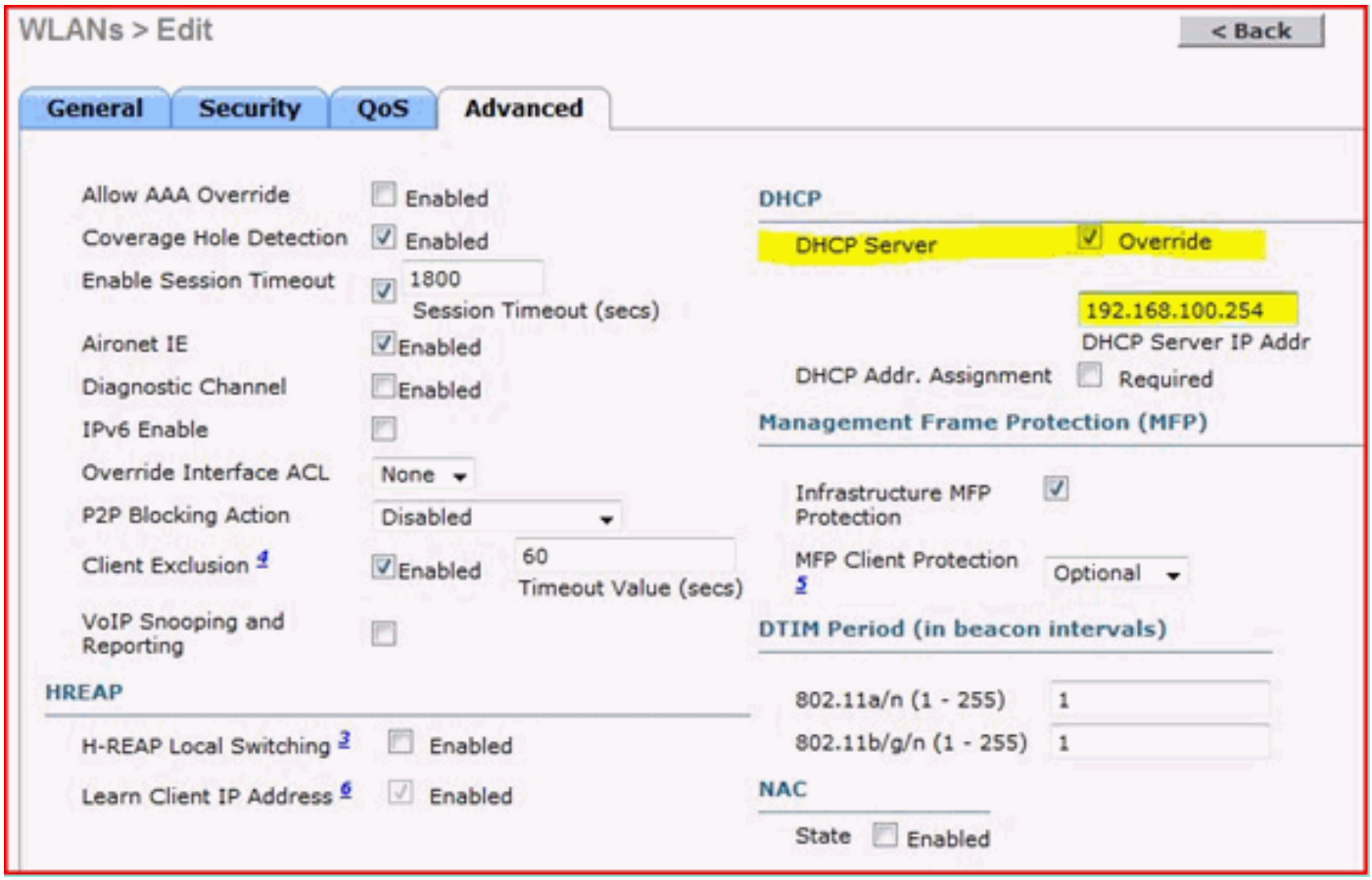
```
Config dhcp proxy enable
Save config
```

내부 DHCP 서버를 활성화하려면 다음 단계를 완료하십시오.

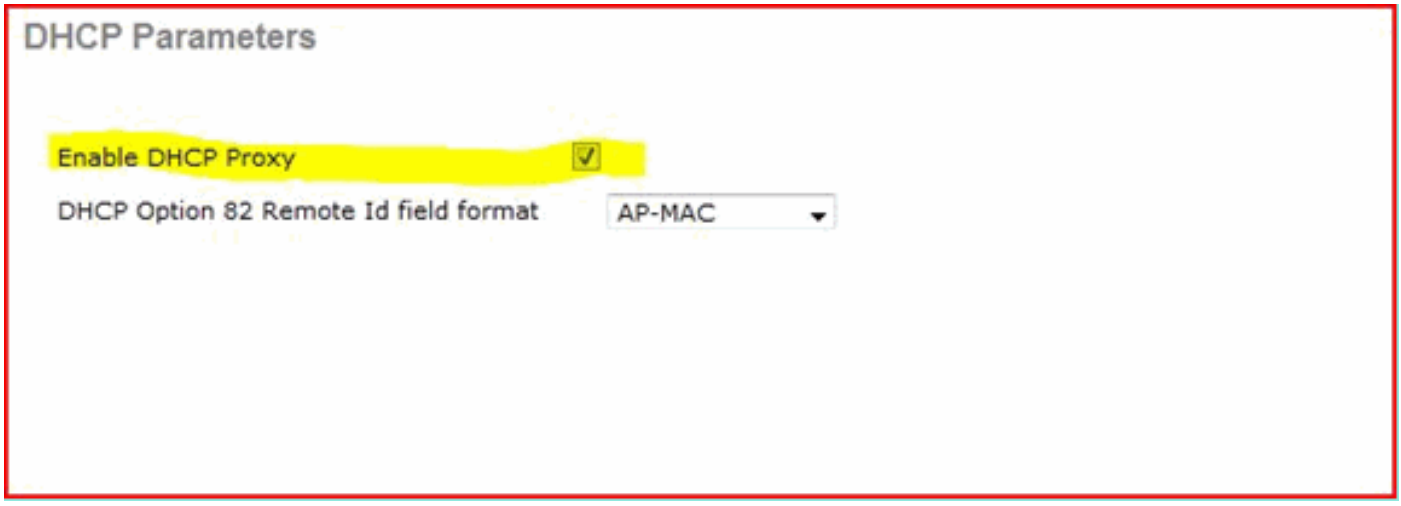
1. IP 주소를 가져오기 위해 사용할 범위를 정의합니다(Controller > Internal DHCP Server > DHCP Scope). 클릭 New.



2. DHCP 재정의를 컨트롤러의 관리 인터페이스 IP 주소로 가리킵니다.



3. DHCP 프록시가 사용하도록 설정되었는지 확인합니다.



문제 해결

내부 DHCP 서버의 디버그는 일반적으로 IP 주소를 얻는 데 문제가 있는 클라이언트를 찾아야 합니다. 이러한 디버그를 실행해야 합니다.

```
debug client <MAC ADDRESS OF CLIENT>
```

디버그 클라이언트는 사용자가 입력한 클라이언트 MAC 주소에만 디버그를 집중시키는 동안 이러한 디버그를 활성화하는 매크로입니다.

```
debug dhcp packet enable
debug dot11 mobile enable
debug dot11 state enable
debug dot1x events enable
debug pem events enable
debug pem state enable
debug cckm client debug enable
```

DHCP 문제의 주요 원인은 debug dhcp packet enable 에서 자동으로 활성화되는 명령 debug client 명령을 실행합니다.

<#root>

00:1b:77:2b:cf:75 dhcpd: received DISCOVER

00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67 from 127.0.0.1:1067

00:1b:77:2b:cf:75 sendto (548 bytes) returned 548
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 312

00:1b:77:2b:cf:75 DHCP option: message type = DHCP OFFER

00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254
00:1b:77:2b:cf:75 DHCP option: lease time = 86400 seconds
00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping
00:1b:77:2b:cf:75 DHCP option: netmask = 255.255.255.0
00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 81

00:1b:77:2b:cf:75 DHCP option: message type = DHCP REQUEST

00:1b:77:2b:cf:75 DHCP option: 61 (len 7) - skipping
00:1b:77:2b:cf:75 DHCP option: requested ip = 192.168.100.100
00:1b:77:2b:cf:75 DHCP option: server id = 192.0.2.10
00:1b:77:2b:cf:75 DHCP option: 12 (len 14) - skipping
00:1b:77:2b:cf:75 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:1b:77:2b:cf:75 DHCP option: 55 (len 11) - skipping
00:1b:77:2b:cf:75 DHCP option: 43 (len 3) - skipping
00:1b:77:2b:cf:75 DHCP options end, len 81, actual 73
00:1b:77:2b:cf:75 DHCP Forwarding packet locally (340 octets) from 192.168.100.254 to 192.168.100.254
dhcpd: Received 340 byte dhcp packet from 0xfe64a8c0 192.168.100.254:68

00:1b:77:2b:cf:75 dhcpd: packet 192.168.100.254 -> 192.168.100.254 using scope "User Scope"

00:1b:77:2b:cf:75 dhcpd: received REQUEST

00:1b:77:2b:cf:75 Checking node 192.168.100.100 Allocated 1246985143, Expires 1247071543 (now: 1246985143)
00:1b:77:2b:cf:75 dhcpd: server_id = c0a864fe
00:1b:77:2b:cf:75 dhcpd: server_id = c0a864fe adding option 0x35 adding option 0x36

```
 adding option 0x33 adding option 0x03 adding option 0x0f adding option 0x01

00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67
  from 127.0.0.1:1067

00:1b:77:2b:cf:75 sendto (548 bytes) returned 548
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 312

00:1b:77:2b:cf:75 DHCP option: message type = DHCP ACK

00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254
00:1b:77:2b:cf:75 DHCP option: lease time = 86400 seconds
00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping
00:1b:77:2b:cf:75 DHCP option: netmask = 255.255.255.0
00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64
```

WLC 내부 DHCP 서버에서 DHCP 임대 지우기

WLC의 내부 DHCP 서버에서 DHCP 임대를 지우려면 다음 명령을 실행할 수 있습니다.

```
<#root>

config dhcp clear-lease
```

예를 들면 다음과 같습니다.

```
<#root>

config dhcp clear-lease all
```

경고

- 내부 DHCP 서버가 작동하려면 DHCP 프록시를 사용하도록 설정해야 합니다.
- CPU ACL의 영향을 받는 내부 DHCP 서버를 사용할 때 포트 1067에 DHCP 사용
- 내부 DHCP 서버는 127.0.0.1 UDP 포트 67을 통해 컨트롤러 루프백 인터페이스에서 수신 대기합니다

최종 사용자 인터페이스

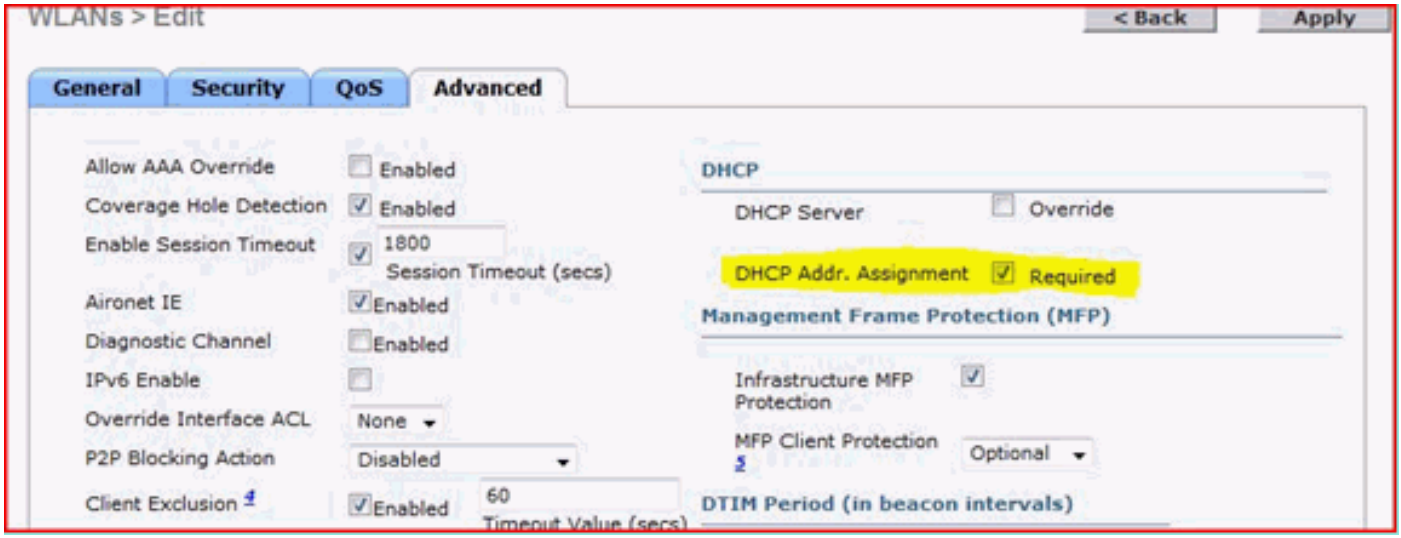
- 이 **config dhcp proxy disable** 명령은 DHCP 브리징 기능의 사용을 의미합니다. 이는 전역 명령입니

다(WLAN별 명령이 아님).

- DHCP 프록시는 기본적으로 활성화되어 있습니다.
- DHCP 프록시가 비활성화되면 로컬 WLAN에서 내부 DHCP 서버를 사용할 수 없습니다. 브리징 작업이 패킷을 내부 서버로 리디렉션하는 데 필요한 작업과 일치하지 않습니다. 브리징은 브리징을 의미합니다. 단, 802.11에서 이더넷 II로 변환하는 경우는 예외입니다. DHCP 패킷은 LWAPP 터널에서 수정되지 않은 상태로 클라이언트 VLAN으로 전달됩니다(또는 그 반대의 경우도 마찬가지임).
- 프록시가 활성화된 경우 WLAN을 활성화하려면 WLAN의 인터페이스(또는 WLAN 자체)에 DHCP 서버를 구성해야 합니다. 프록시가 비활성화되면 이러한 서버가 사용되지 않으므로 서버를 구성할 필요가 없습니다.
- 사용자가 DHCP 프록시를 활성화하려고 하면 모든 WLAN(또는 연결된 인터페이스)에 DHCP 서버가 구성되어 있는지 내부적으로 확인합니다. 그렇지 않으면 활성화 작업이 실패합니다.

DHCP 필요

WLAN 고급 컨피그레이션에는 사용자가 RUN 상태(클라이언트가 컨트롤러를 통해 트래픽을 전달할 수 있는 상태)로 전환하기 전에 DHCP를 전달해야 하는 옵션이 있습니다. 이 옵션을 사용하려면 클라이언트에서 전체 또는 절반의 DHCP 요청을 수행해야 합니다. 컨트롤러가 클라이언트에서 주로 찾는 것은 DHCP 요청과 DHCP 서버에서 반환되는 ACK입니다. 클라이언트가 이러한 단계를 수행하는 동안 클라이언트는 DHCP 필수 단계를 통과하고 RUN 상태로 이동합니다.



L2 및 L3 로밍

L2 Roam - 클라이언트에 유효한 DHCP 리스가 있고 동일한 L2 네트워크에 있는 두 개의 다른 컨트롤러 간에 L2 로밍을 수행하는 경우, 클라이언트는 DHCP를 다시 수행할 필요가 없으며 클라이언트 항목은 원래 컨트롤러에서 새 컨트롤러로 완전히 이동해야 합니다. 그런 다음 클라이언트에서 다시 DHCP를 수행해야 하는 경우 현재 컨트롤러의 DHCP 브리징 또는 프록시 프로세스에서 패킷을 투명하게 다시 브리징합니다.

L3 Roam - L3 Roam 시나리오에서 클라이언트는 서로 다른 L3 네트워크의 서로 다른 두 컨트롤러 사이를 이동합니다. 이러한 상황에서 클라이언트는 원래 컨트롤러에 고정되며 새 외부 컨트롤러의 클라이언트 테이블에 나열됩니다. 앵커 시나리오 동안 클라이언트 데이터가 외부 컨트롤러와 앵커 컨트롤러 간의 EoIP 터널 내에서 터널링되므로 클라이언트 DHCP는 앵커 컨트롤러에 의해 처리됩니다.

관련 정보

- 경량형 Cisco Aironet Access Point용 DHCP 옵션 43 설정 예
- 기술 지원 및 문서 − Cisco Systems

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.