

# AireOS WLCによるDHCPプロトコルの処理方法の理解

## 内容

---

### [はじめに](#)

#### [外部 DHCP サーバ](#)

[DHCP プロキシとブリッジ モードの比較](#)

[DHCP プロキシ モード](#)

[プロキシ パケットのフロー](#)

[プロキシ パケットのキャプチャ](#)

[クライアント側](#)

[サーバ側](#)

[プロキシの設定例](#)

[トラブルシューティング](#)

[警告](#)

#### [DHCP ブリッジ モード](#)

[DHCP ブリッジの動作：ブリッジ パケット フロー](#)

[ブリッジ パケットのキャプチャ：クライアント側](#)

[ブリッジ パケットのキャプチャ：サーバ側](#)

[ブリッジの設定例](#)

[トラブルシューティング](#)

[警告](#)

#### [内部 DHCP サーバ](#)

[内部 DHCP とブリッジ モードの比較](#)

[内部 DHCP サーバ：パケット フロー](#)

[内部 DHCP サーバの設定例](#)

[トラブルシューティング](#)

[WLC内部DHCPサーバでのDHCPリースのクリア](#)

[警告](#)

#### [エンド ユーザ インターフェイス](#)

#### [DHCP 要求](#)

#### [L2 と L3 のローミング](#)

#### [関連情報](#)

---

## はじめに

このドキュメントでは、Cisco AireOSワイヤレスコントローラのさまざまなDHCP操作について説明します。

## 外部 DHCP サーバ

外部 DHCP サーバを使用する場合、ワイヤレス LAN コントローラ ( WLC ) では DHCP の次の 2 つの動作モードがサポートされます。

- DHCP プロキシ モード
- DHCP ブリッジモード

DHCP プロキシモードは DHCP ヘルパー機能として動作し、DHCP サーバとワイヤレスクライアントの間の DHCP トランザクションのセキュリティと制御を強化します。DHCPブリッジモードには、DHCPトランザクションでのコントローラの役割をワイヤレスクライアントに対して完全に透過的にするオプションがあります。

## DHCP プロキシとブリッジ モードの比較

クライアント DHCP の処理	DHCP プロキシ モード	DHCP ブリ ッジ モード
giaddr の変更	Yes	いいえ
siaddr の変更	Yes	いいえ
パケットの内容の 変更	Yes	いいえ
冗長オフアーは転 送されない	Yes	いいえ
オプション 82 の サポート	Yes	いいえ
ブロードキャスト からユニキャスト へ	Yes	いいえ
BOOTP のサポー ト	いいえ	サーバ
RFC 非準拠	プロキシエージェントとリレーエージェントは、まったく同じ概念ではありません。RFC に完全に準拠するには、DHCP ブリッジ モードを推奨します。	いいえ

## DHCP プロキシ モード

DHCP プロキシはすべてのネットワーク環境に最適であるとは限りません。コントローラは、ヘルパー機能を提供し、特定のセキュリティ問題に対処するために、すべてのDHCPトランザクションを変更およびリレーします。


通常、コントローラの仮想IPアドレスは、クライアントに対するすべてのDHCPトランザクションの送信元IPアドレスとして使用されます。その結果、実際の DHCP サーバ IP アドレスが公表されることはありません。この仮想 IP はコントローラ上で、DHCP トランザクションのデバッ

グ出力として表示されます。ただし、仮想IPアドレスを使用すると、特定のタイプのクライアントで問題が発生する可能性があります。

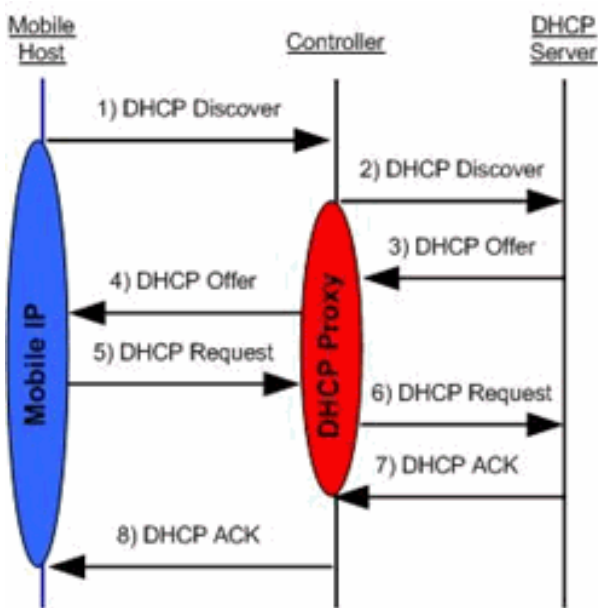
DHCPプロキシモードの動作では、対称モビリティプロトコルと非対称モビリティプロトコルの両方で同じ動作が維持されます。

外部 DHCP サーバから複数のオファーが着信すると、通常 DHCP プロキシは着信した最初のオファーを選択して、そのサーバの IP アドレスをクライアントのデータ構造に設定します。その結果、再試行後にトランザクションが失敗するまで、後続のすべてのトランザクションは同じ DHCPサーバを介して実行されます。この時、プロキシはクライアントに異なる DHCP サーバを選択します。

DHCP プロキシはデフォルトでイネーブルです。通信するすべてのコントローラは、同じ DHCPプロキシ設定を持つ必要があります。

 注:DHCPオプション82が正しく動作するには、DHCPプロキシを有効にする必要があります。

## プロキシ パケットのフロー



### Handling of Packets for Local Clients

- 1) Client sends DHCP discover as all-subnets broadcast
- 2) Controller unicasts DHCP discover to DHCP servers configured on WLAN with WLAN IP address as source
- 3) DHCP server sends DHCP offer to controller (only first offer received by controller is processed. All others are dropped by proxy)
- 4) Controller unicasts DHCP offer to client with option 54 and source address set as controller's virtual IP (clients now believes controller is DHCP server)
- 5) Client sends DHCP request to virtual IP address
- 6) Controller unicasts DHCP request from WLAN IP address to DHCP server which returned the first offer to the client
- 7) DHCP server send ACK to controller
- 8) Controller unicasts ACK from the virtual IP to the client

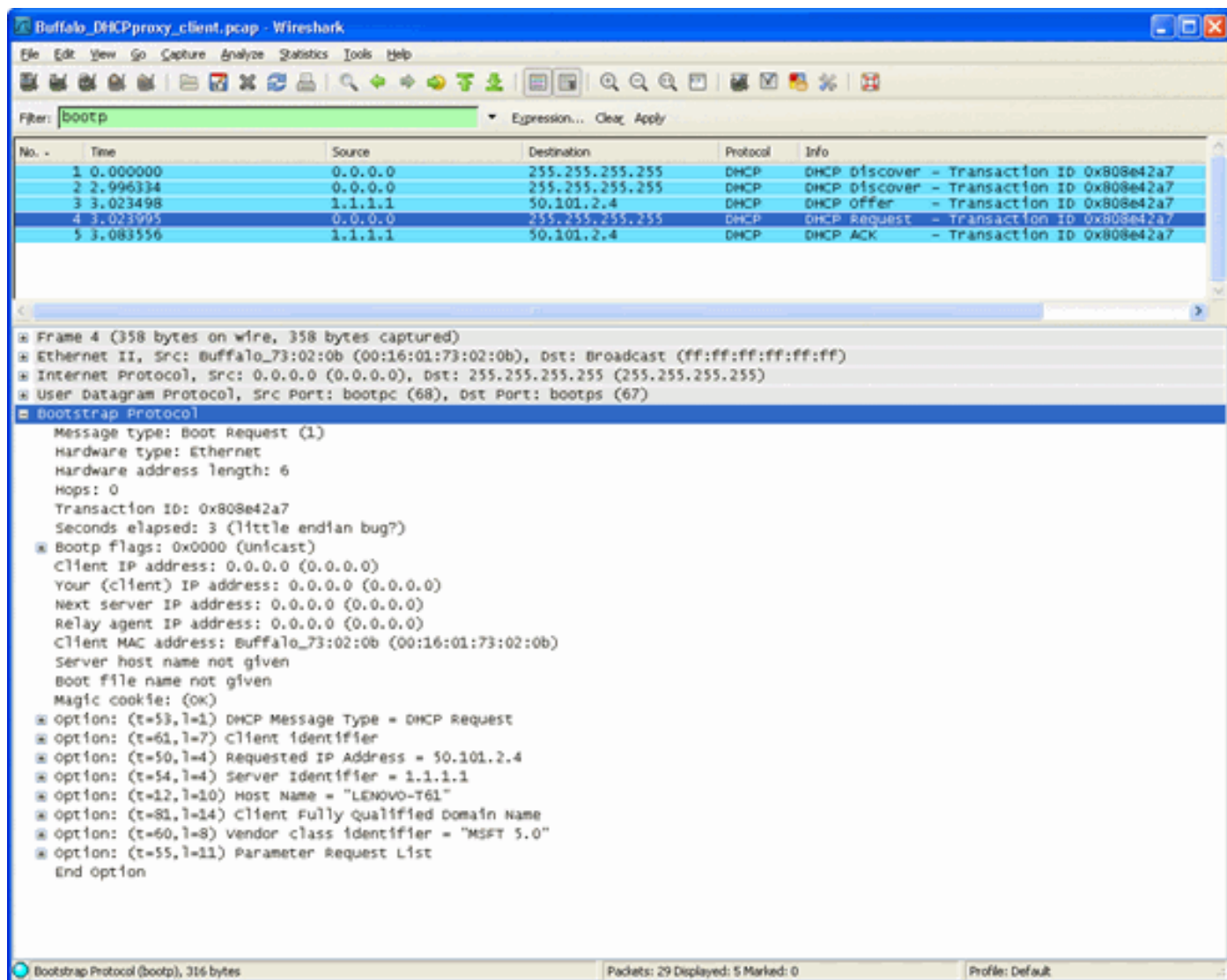
## プロキシ パケットのキャプチャ

コントローラが DHCP プロキシモードの場合、コントローラは DHCP パケットを DHCP サーバに送信するだけでなく、実際に新しい DHCP パケットを作成して、DHCP サーバに転送します。クライアントDHCPパケットに存在するすべてのDHCPオプションは、コントローラDHCPパケットにコピーされます。次のスクリーンショットには、DHCP Request パケットの例が示されています。

### クライアント側

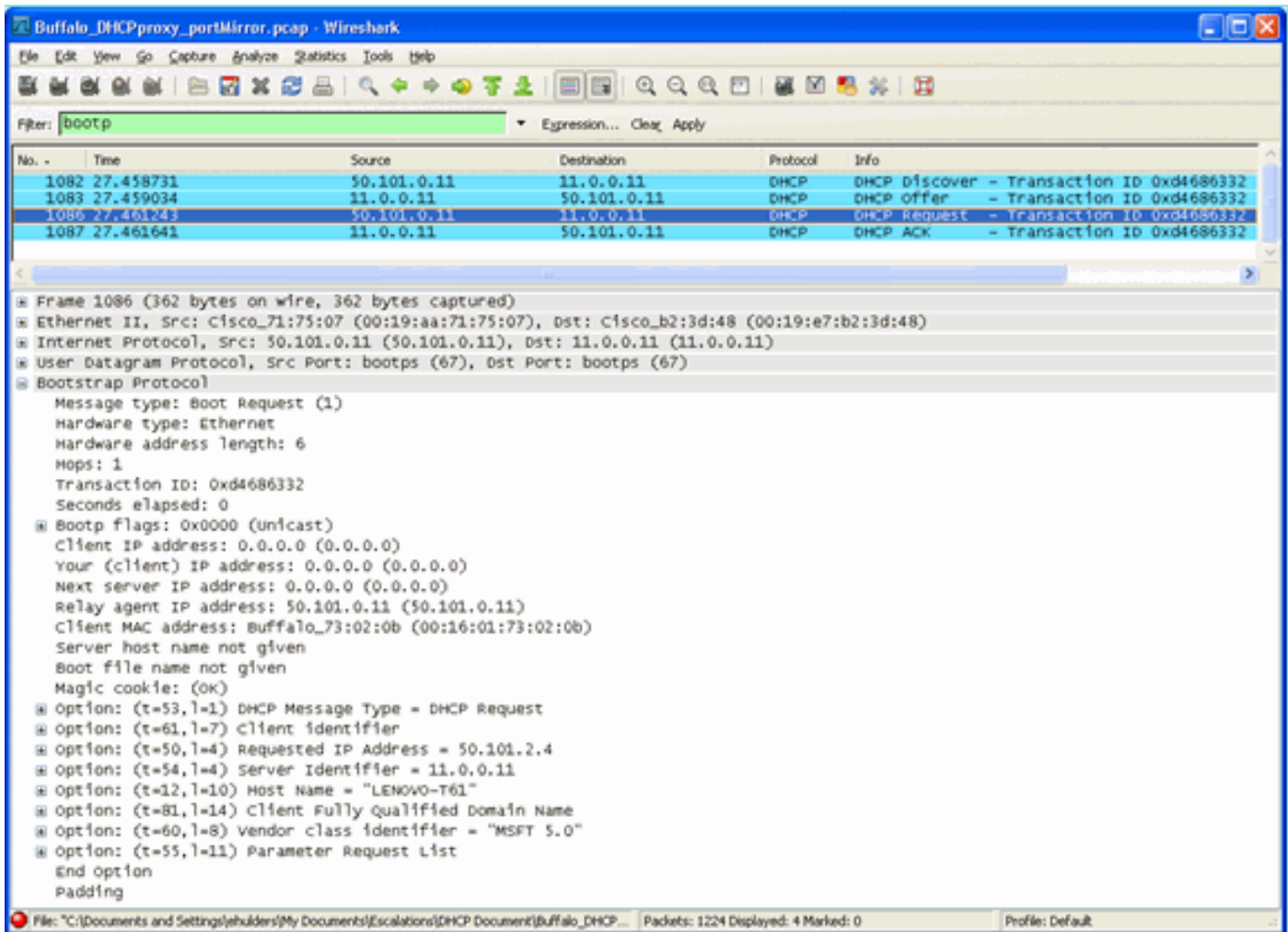
このスクリーンショットは、クライアント側から見たパケットキャプチャです。ここには、

DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK が示されています。DHCP要求が強調表示され、boot pの詳細が展開されて、DHCPオプションが表示されます。



### サーバ側

このスクリーンショットは、サーバ側から見たパケットキャプチャです。前の例と同様、DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK が示されています。ただし、これらはコントローラがDHCPプロキシの機能として構築したパケットです。ここでも、DHCP要求が強調表示され、boot pの詳細が展開されて、DHCPオプションが表示されます。これらはクライアントのDHCP要求パケットと同じであることを注意してください。また、WLCプロキシがパケットをリレーし、パケットアドレスを強調表示することに注意してください。



## プロキシの設定例

コントローラを DHCP プロキシとして使用するには、コントローラで DHCP プロキシ機能をイネーブルにする必要があります。デフォルトでは、この機能はイネーブルです。DHCP プロキシを有効にするには、次の CLI コマンドを使用できます。GUI の DHCP メニューのコントローラページでも同じことができます。

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy enable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

DHCP プロキシが動作するには、DHCP サービスを必要とする各コントローラインターフェイスでプライマリ DHCP サーバを設定する必要があります。DHCP サーバは、管理インターフェイス、ap マネージャインターフェイス、およびダイナミックインターフェイスで設定できます。次の CLI コマンドを使用して、各インターフェイスに DHCP サーバを設定することができます。

<#root>

(Cisco Controller) >

```
config interface dhcp ap-manager primary <primary-server>
```

(Cisco Controller) >

```
config interface dhcp management primary <primary-server>
```

(Cisco Controller) >

```
config interface dhcp dynamic-interface <interface-name>
```

```
primary <primary-server>
```

DHCP ブリッジ機能はグローバル設定であるため、コントローラ内のすべての DHCP トランザクションに影響します。

トラブルシューティング

このコマンドの出力を示します。 `debug dhcp packet enable` デバッグには、コントローラが MAC アドレス 00:40:96:b4:8c:e1 のクライアントから DHCP Request を受信し、DHCP Request を DHCP サーバに送信し、DHCP サーバからの応答を受信し、DHCP Offer をクライアントに送信していることが示されています。

<#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
```

```
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
```

```
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
```

```
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 - cont
```

```
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
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 mob
```

```
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 21:48:5

## 警告

•

DHCP プロキシがイネーブルになっているコントローラと、ファイアウォールと DHCP サーバの両方として機能するデバイスの間には、相互運用性の問題がある可能性があります。この問題の主な原因は、一般にファイアウォールとして使用されるデバイスのファイアウォール コンポーネントがプロキシ要求に応答しないためです。この問題の回避策は、コントローラでDHCPプロキシを無効にすることです。

•

クライアントがコントローラでDHCP REQ状態になると、コントローラはDHCP informパケットをドロップします。クライアントは、クライアントからDHCP Discoverパケットを受信するまで、コントローラ上でRUN状態にはなりません (これはクライアントがトラフィックを渡すために必要です)。DHCPプロキシが無効になると、DHCPインフォームパケットがコントローラによって転送されます。

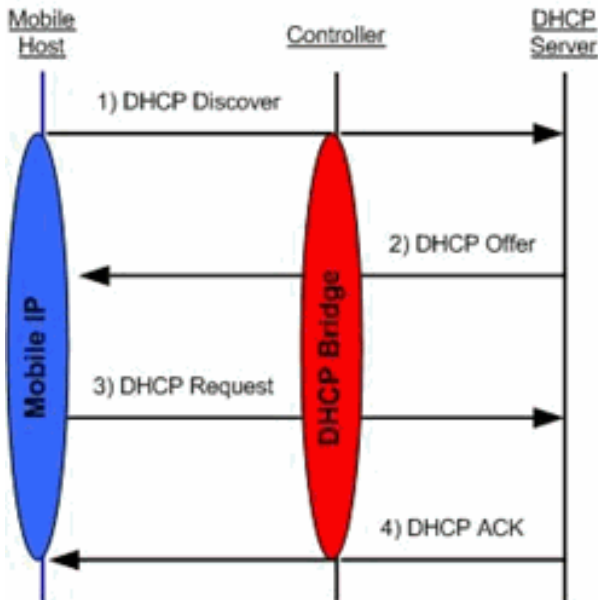
•

相互に通信するすべてのコントローラは、同じDHCPプロキシ設定を持つ必要があります。

## DHCP ブリッジ モード

DHCPブリッジ機能は、DHCPトランザクションでのコントローラの役割をクライアントに対して完全に透過的にするように設計されています。802.11からイーサネットIIへの変換を除き、クライアントからのパケットはLight Weight Access Point Protocol(LWAPP)トンネルからクライアントVLAN(またはL3ローミングの場合はEthernet over IP(EoIP)トンネル)へ、変更されずにブリッジされます。同様に、イーサネットIIから802.11への変換を除き、クライアントへのパケットはクライアントVLAN (またはL3ローミングの場合はEoIPトンネル) からLWAPPトンネルへ、変更されずにブリッジされます。これは、クライアントをスイッチポートに書き込み、そのクライアントが従来の DHCP トランザクションを実行することと同様であると見なすことができます。

DHCP ブリッジの動作 : ブリッジ パケット フロー



### Handling of Packets for Local Clients

- 1) Client sends DHCP discover as all-subnets broadcast which is bridged by the controller.
- 2) DHCP server sends DHCP offer to client in a unicast packet.
- 3) Client sends DHCP request as all-subnets broadcast which is bridged by the controller.
- 4) DHCP server send ACK to client in a unicast packet.

ブリッジパケットのキャプチャ：クライアント側

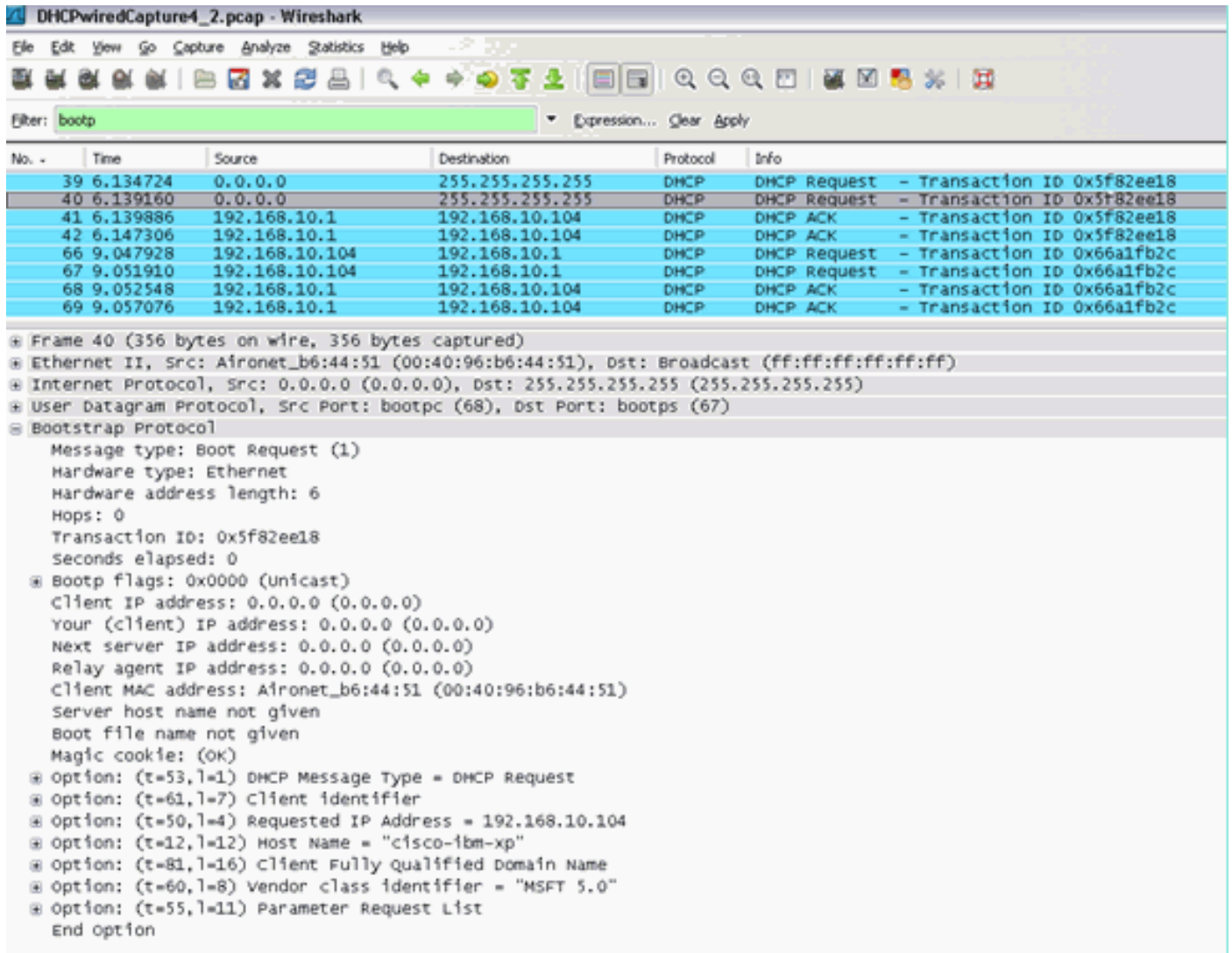
Wireshark capture details for a DHCP Offer packet:

- Frame 8 (342 bytes on wire, 342 bytes captured)
- Ethernet II, Src: Cisco\_32:7a:40 (00:1a:e3:32:7a:40), Dst: 00:1b:77:23:96:8a (00:1b:77:23:96:8a)
- Internet Protocol, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.120 (192.168.10.120)
- User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
- Bootstrap Protocol
  - Message type: Boot Reply (2)
  - Hardware type: Ethernet
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0x498ae625
  - Seconds elapsed: 0
  - Bootp flags: 0x0000 (unicast)
  - Client IP address: 0.0.0.0 (0.0.0.0)
  - Your (client) IP address: 192.168.10.120 (192.168.10.120)
  - Next server IP address: 0.0.0.0 (0.0.0.0)
  - Relay agent IP address: 0.0.0.0 (0.0.0.0)
  - Client MAC address: 00:1b:77:23:96:8a (00:1b:77:23:96:8a)
  - Server host name not given
  - Boot file name not given
  - Magic cookie: (ok)
  - Option: (t=53,l=1) DHCP Message Type = DHCP offer
  - Option: (t=54,l=4) Server Identifier = 192.168.10.1
  - Option: (t=51,l=4) IP Address Lease Time = 1 day
  - Option: (t=58,l=4) Renewal Time value = 12 hours
  - Option: (t=59,l=4) Rebinding Time value = 21 hours
  - Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  - Option: (t=3,l=4) Router = 192.168.10.1
  - End option

クライアント側のパケットキャプチャのスクリーンショットでは、プロキシモードでのクライアントキャプチャの主な違いは、コントローラの仮想IPアドレスではなく、OfferパケットとAckパケットに表示されるDHCPサーバの実際のIPです。



## ブリッジパケットのキャプチャ：サーバ側



No.	Time	Source	Destination	Protocol	Info
39	6.134724	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x5f82ee18
40	6.139160	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x5f82ee18
41	6.139886	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x5f82ee18
42	6.147306	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x5f82ee18
66	9.047928	192.168.10.104	192.168.10.1	DHCP	DHCP Request - Transaction ID 0x66a1fb2c
67	9.051910	192.168.10.104	192.168.10.1	DHCP	DHCP Request - Transaction ID 0x66a1fb2c
68	9.052548	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x66a1fb2c
69	9.057076	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x66a1fb2c

```
⊕ Frame 40 (356 bytes on wire, 356 bytes captured)
⊕ Ethernet II, Src: Aironet_b6:44:51 (00:40:96:b6:44:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊕ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊕ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊖ Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x5f82ee18
  Seconds elapsed: 0
  ⊕ Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Aironet_b6:44:51 (00:40:96:b6:44:51)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
  ⊕ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ⊕ Option: (t=61,l=7) Client identifier
  ⊕ Option: (t=50,l=4) Requested IP Address = 192.168.10.104
  ⊕ Option: (t=12,l=12) Host Name = "cisco-ibm-xp"
  ⊕ Option: (t=81,l=16) Client Fully Qualified Domain Name
  ⊕ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊕ Option: (t=55,l=11) Parameter Request List
  End Option
```

有線パケットキャプチャのスクリーンショットでは、パケット 40 がテストクライアント 00:40:96:b6:44:51 から有線ネットワークへの DHCP Request ブロードキャストであることが示されています。

## ブリッジの設定例

DHCP ブリッジ機能をコントローラでイネーブルにするには、コントローラで DHCP プロキシ機能をディセーブルにする必要があります。この機能をディセーブルにするには、CLI で次のコマンドを使用する必要があります。

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy disable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behaviour: disabled
```

DHCPサーバがクライアントと同じレイヤ2(L2)ネットワークに存在しない場合は、IPヘルパーを使用して、クライアントゲートウェイのDHCPサーバにブロードキャストを転送する必要があります。次に、この設定の例を示します。

```
<#root>
```

```
Switch#
```

```
conf t
```

```
Switch(config)#
```

```
interface vlan <client vlan #>
```

```
Switch(config-if)#
```

```
ip helper-address <dhcp server IP>
```

DHCPブリッジ機能はグローバル設定であるため、コントローラ内のすべてのDHCPトランザクションに影響します。コントローラ上の必要なすべてのVLANについて、有線インフラストラクチャにIP helper文を追加する必要があります。

トラブルシュート

ここに一覧で表示されているデバッグはコントローラ CLI でイネーブルにされ、このドキュメント用に出力のDHCPの部分が抜粋されています。

```
<#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 DHC
```

```
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 DHC
```

```
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) -
```

```
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 DHC
```

```
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 DHC
```

```
00:40:96:b6:44:51 Assigning Address 192.168.10.104 to mobile 00:40:96:b6:44:51 DHCP successfully bridged
```

この DHCP デバッグ出力には、コントローラで DHCP ブリッジが使用されていることを示すいくつかの点があります。

- DHCP successfully bridged packet to DS : クライアントから送信された元の DHCP パケットは変更されずに配信システム ( DS ) にブリッジされたことを示します。DS は有線のインフラストラクチャです。
- DHCP successfully bridged packet to STA : このメッセージは、DHCP パケットは変更されずにステーション ( STA ) にブリッジされたことを示します。STA は DHCP を要求するクライアントマシンです。

また、デバッグには実際のサーバ IP アドレスが表示されています。これは 192.168.10.1 です。DHCPブリッジの代わりに DHCPプロキシを使用している場合は、サーバのIPアドレスに対応するコントローラの仮想IPアドレスが表示されます。

## 警告

- デフォルトでは、DHCPプロキシは有効になっています。
- 相互に通信するすべてのコントローラは、同じDHCPプロキシ設定を持つ必要があります。
- DHCP オプション 82 が動作するには、DHCP プロキシがイネーブルになっている必要があります。

## 内部 DHCP サーバ

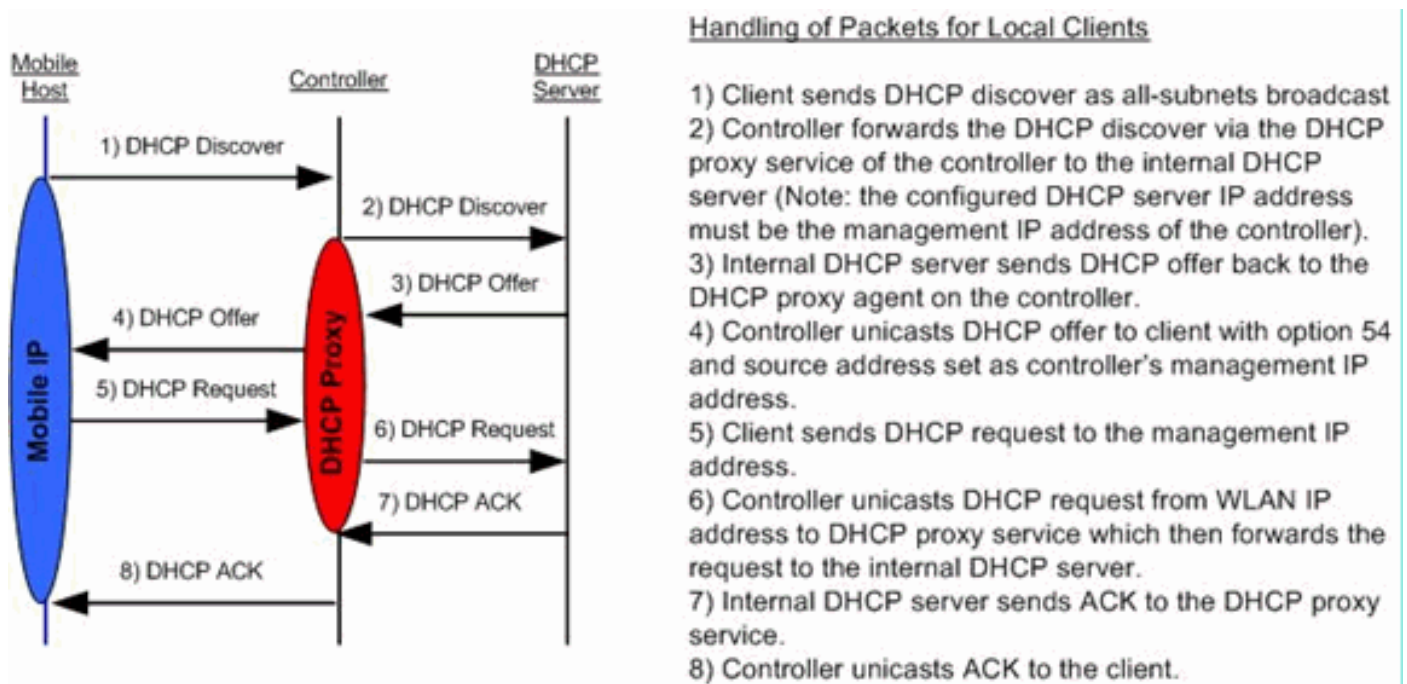
内部 DHCP サーバは、外部 DHCP サーバを使用できないブランチ オフィス用に当初から導入されていました。同じサブネット上にある10未満のアクセスポイント(AP)を持つ小規模なワイヤレスネットワークをサポートするために設計されています。内部サーバは、ワイヤレス クライアント、直接接続 AP、管理インターフェイスのアプライアンス モード AP、および AP から中継される DHCP 要求に対し、IP アドレスを提供します。これは、本格的な汎用DHCPサーバではありません。サポートする機能は限られており、大規模な導入では拡張できません。

## 内部 DHCP とブリッジ モードの比較

コントローラの主要な 2 つの DHCP モードは、DHCP プロキシまたは DHCP ブリッジのいずれかです。DHCP ブリッジを使用すると、コントローラは自律型 AP による DHCP Back のように機能します。DHCP パケットは、VLAN にリンクされているサービスセット識別子 ( SSID ) へのクライアント関連付けから AP に送信されます。次に、DHCP パケットはその VLAN から送信されます。IPヘルパーがそのVLANのレイヤ3(L3)ゲートウェイで定義されている場合、パケットはダイレクトユニキャストを介してそのDHCPサーバに転送されます。次に、DHCP サーバは、その DHCP パケットを転送した L3 インターフェイスに直接応答を返します。DHCPプロキシでも同じ考えですが、すべての転送はVLANのL3インターフェイスではなく、コントローラで直接行われます。たとえば、クライアントからWLANにDHCP要求が着信すると、WLANでは、VLANのインターフェイスで定義されている

DHCPサーバを使用するか、またはWLANのDHCPオーバーライド機能を使用して、DHCPパケットのGIADDRフィールドにVLANインターフェイスのIPアドレスを入力して、ユニキャストDHCPパケットをDHCPサーバに転送します。

内部 DHCP サーバ : パケット フロー

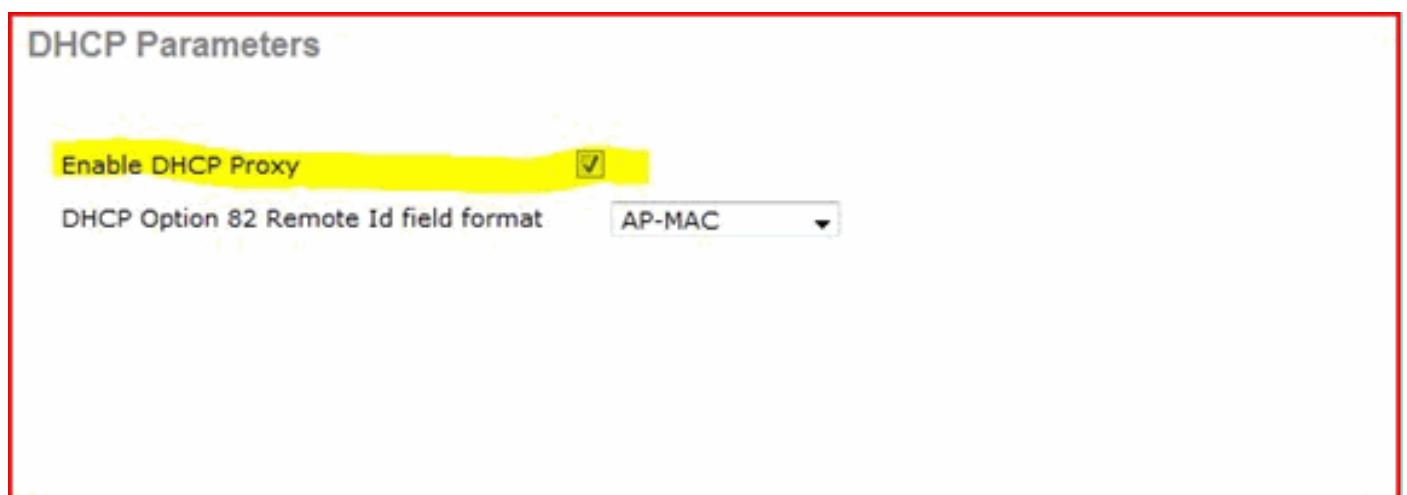


内部 DHCP サーバの設定例

内部DHCPサーバが機能できるようにするには、コントローラでDHCPプロキシを有効にする必要があります。これは、次のセクションにある GUI から行うことができます。

 注：すべてのバージョンで、GUI経由でDHCPプロキシを設定することはできません。

Controller->Advanced->DHCP



または、次のように CLI から行うことができます。

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

内部 DHCP サーバをイネーブルにするには、次の手順を実行します。

1. IPアドレスをプルするために使用するスコープを定義します(Controller > Internal DHCP Server > DHCP Scope)。をクリックします。  
。 New

### DHCP Scope > Edit

Scope Name	User Scope		
Pool Start Address	<input type="text" value="192.168.100.100"/>		
Pool End Address	<input type="text" value="192.168.100.200"/>		
Network	<input type="text" value="192.168.100.0"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
Lease Time (seconds)	<input type="text" value="86400"/>		
Default Routers	<input type="text" value="192.168.100.1"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
DNS Domain Name	<input type="text" value="wlc2106.local"/>		
DNS Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Netbios Name Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Status	<input type="text" value="Enabled"/> ▼		

2. DHCPオーバーライドをコントローラの管理インターフェイスIPアドレスにポイントします。

WLANs > Edit < Back

**General** **Security** **QoS** **Advanced**

Allow AAA Override  Enabled  
 Coverage Hole Detection  Enabled  
 Enable Session Timeout  1800  
     Session Timeout (secs)  
 Aironet IE  Enabled  
 Diagnostic Channel  Enabled  
 IPv6 Enable   
 Override Interface ACL   
 P2P Blocking Action   
 Client Exclusion  Enabled 60  
     Timeout Value (secs)  
 VoIP Snooping and Reporting

**DHCP**

DHCP Server  Override  
 192.168.100.254  
 DHCP Server IP Addr  
 DHCP Addr. Assignment  Required

**Management Frame Protection (MFP)**

Infrastructure MFP Protection   
 MFP Client Protection

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255)   
 802.11b/g/n (1 - 255)

**HREAP**

H-REAP Local Switching  Enabled  
 Learn Client IP Address  Enabled

**NAC**

State  Enabled

3. DHCPプロキシが有効になっていることを確認します。

**DHCP Parameters**

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

トラブルシュート

内部DHCPサーバのデバッグでは通常、IPアドレスの取得に問題のあるクライアントを見つける必要があります。次のデバッグを実行する必要があります。

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

debug client は、入力したクライアント MAC アドレスのみでデバッグをイネーブルにするマクロです。

debug dhcp packet enable debug dot11 mobile enable debug dot11 state enable debug dot1x events enable debug pem events enable debug pem state enable

DHCPが発行する主なコマンドは、debug clientコマンドによって自動的にイネーブルになるdebug dhcp packet enableコマンドです。

<#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 mag
```

```
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 =
```

```
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
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 = c
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 mag
```

```
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 =
```

WLC内部DHCPサーバでのDHCPリースのクリア

次のコマンドを発行して、WLC の内部 DHCP サーバにある DHCP リースをクリアできます。

<#root>

```
config dhcp clear-lease <all/IP Address>
```

ランダム データの例は次のとおりです。

```
<#root>
```

```
config dhcp clear-lease all
```

#### 警告

- 内部DHCPサーバが機能するためには、DHCPプロキシをイネーブルにする必要があります
- 内部DHCPサーバを使用する場合のポート1067へのDHCPの使用 ( CPU ACLの影響を受ける )
- 内部DHCPサーバは、127.0.0.1 UDPポート67を介してコントローラループバックインターフェイスでリッスンします

#### エンド ユーザ インターフェイス

- **config dhcp proxy disable** コマンドは、DHCPブリッジ機能を使用します。これはグローバル コマンドです ( WLAN ごとのコマンドではありません )。
- DHCPプロキシはデフォルトで有効になっています。
-



DHCP プロキシをディセーブルにすると、ローカル WLAN は内部 DHCP サーバを使用できません。ブリッジ動作は、パケットを内部サーバにリダイレクトするために必要な動作と同じにはなりません。ブリッジは、802.11 からイーサネット II への変換を除き、単にブリッジするだけとなります。DHCP パケットは、変更されずに LWAPP トンネルからクライアント VLAN に ( またはその逆に ) 渡されます。

•

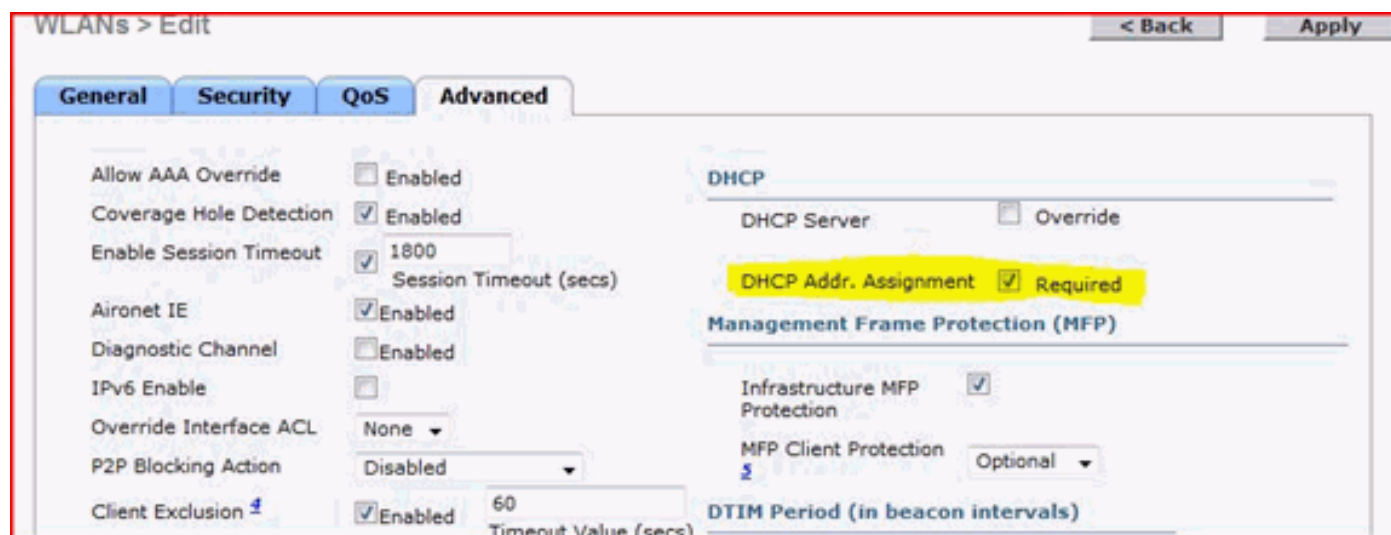
プロキシをイネーブルにする場合、WLAN をイネーブルにするには、DHCP サーバを WLAN のインターフェイス ( または WLAN 自体 ) で設定する必要があります。プロキシがディセーブルのときには、サーバは使用されないため、サーバを設定する必要はありません。

•

ユーザが DHCP プロキシをイネーブルにしようとすると、すべての WLAN ( または関連付けられているインターフェイス ) に DHCP サーバが設定されていることを内部で確認します。設定されていないと、イネーブル動作は失敗します。

## DHCP 要求

WLAN の高度な設定には、RUN 状態 ( クライアントがコントローラを介してトラフィックを渡すことができる状態 ) に移行する前にユーザに DHCP を渡すように要求するオプションがあります。このオプションでは、DHCP Request の全部または半分をクライアントに要求します。クライアントからコントローラに提示される主要なものは、DHCP Request と DHCP サーバから戻される ACK です。クライアントがこれらの手順を実行している限り、クライアントは DHCP の必須の手順を通過し、RUN 状態に移行します。



## L2 と L3 のローミング

L2 Roam: クライアントに有効な DHCP リースがあり、同じ L2 ネットワーク上の 2 つの異なるコントローラ間で L2 ローミングを実行する場合、クライアントで reDHCP を実行する必要はなく、クライアント エントリを完全に元のコントローラから新しいコントローラに移動する必要があります。次に、クライアントが再び DHCP を必要とする場合、現在のコントローラ上の DHCP ブリッジングまたはプロキシプロセスは、再びパケットを透過的にブリッジします。

ローミング:L3ローミングのシナリオでは、クライアントは異なるL3ネットワークにある2つの異なるコントローラ間を移動します。この場合、クライアントは元のコントローラにアンカーされ、新しい外部コントローラのクライアントテーブルにリストされます。アンカーシナリオでは、クライアントデータは外部コントローラとアンカーコントローラ間のEoIPトンネル内でトンネリングされるため、クライアントのDHCPはアンカーコントローラで処理されます。

#### 関連情報

- [Lightweight Cisco Aironet アクセス ポイント用 DHCP オプション 43 の設定例](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 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。