瞭解AireOS WLC如何處理DHCP協定

目錄

簡介

本文檔介紹Cisco AireOS無線控制器上的不同DHCP操作。

外部DHCP伺服器

在使用外部DHCP伺服器時，無線LAN控制器(WLC)支援兩種DHCP作業模式：

- DHCP代理模式
- DHCP橋接模式

DHCP代理模式用作DHCP幫助功能，以便在DHCP伺服器和無線客戶端之間實現更好的安全性和對DHCP事務的控制。DHCP橋接模式提供了使控制器角色在DHCP事務中對無線客戶端完全透明的選項。

DHCP代理和橋接模式的比較

處理客戶端DHCP	DHCP代理模式	DHCP橋接模式
修改giaddr	是	否
修改siaddr	是	否
修改資料包內容	是	否
未轉發冗餘產品	是	否
選項82支援	是	否
廣播到單播	是	否
BOOTP支援	否	伺服器
RFC不符合	代理和中繼代理的概念不完全相同。建議使用DHCP橋接模式以完全符合RFC。	否

DHCP代理模式

DHCP代理並非適用於所有網路環境。控制器修改並中繼所有DHCP事務，以提供幫助功能和解決某些安全問題。

控制器虛擬IP地址通常用作客戶端的所有DHCP事務的源IP地址。因此，實際DHCP伺服器IP地址不會暴露在空中。此虛擬IP顯示在控制器上DHCP事務的調試輸出中。但是，使用虛擬IP地址可能會導致某些型別的客戶端出現問題。

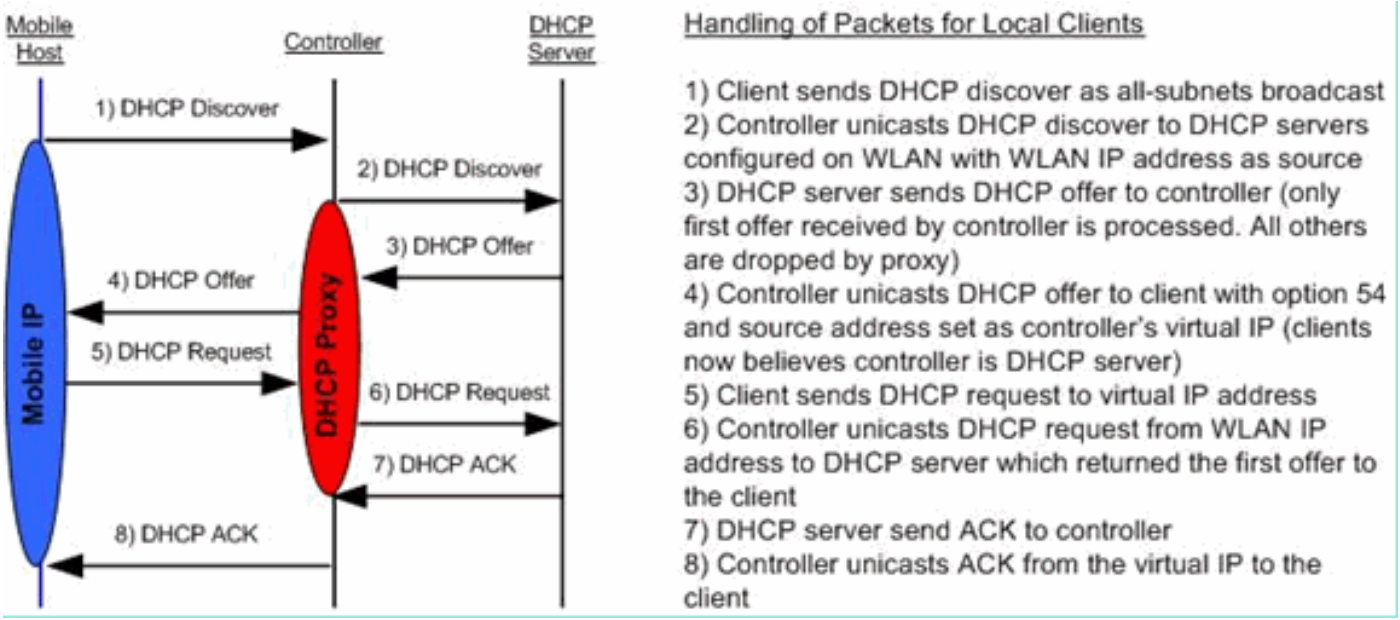
對於對稱和非對稱移動協定，DHCP代理模式操作保持相同的行為。

當多個產品來自外部DHCP伺服器時，DHCP代理通常會選擇第一個產品，並在客戶端資料結構中設定伺服器的IP地址。因此，所有後續事務都通過同一個DHCP伺服器運行，直到事務在重試後失敗。此時，代理為客戶端選擇不同的DHCP伺服器。

預設情況下啟用DHCP代理。所有進行通訊的控制器必須具有相同的DHCP代理設定。

註：必須啟用DHCP代理，DHCP選項82才能正常運行。

代理資料包流

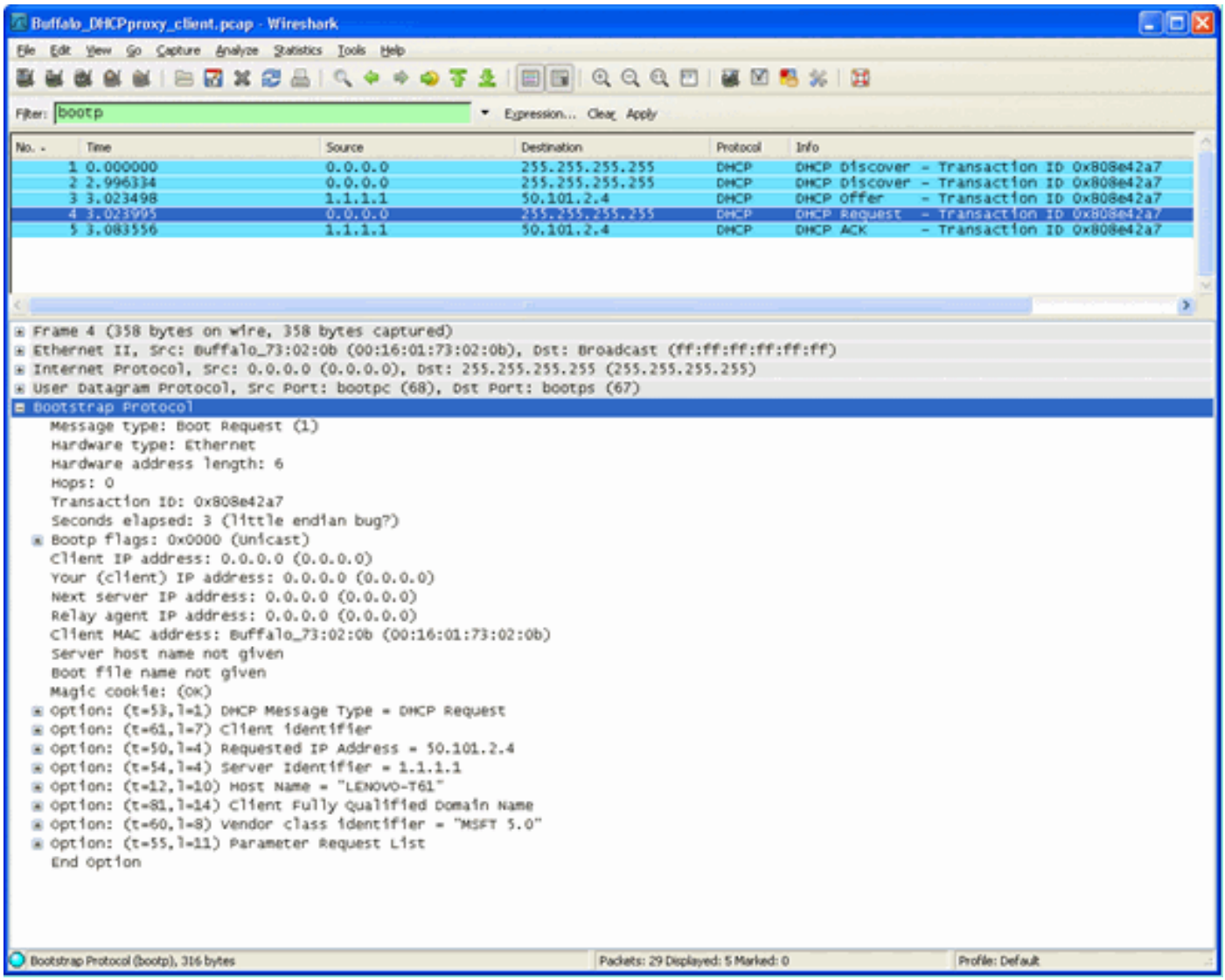


代理資料包捕獲

當控制器處於DHCP代理模式時，它不僅會將DHCP資料包定向到DHCP伺服器，還會實際構建新的DHCP資料包以轉發到DHCP伺服器。客戶端DHCP資料包中存在的所有DHCP選項均複製到控制器DHCP資料包中。下一個螢幕截圖示例顯示了有關DHCP請求資料包的此類資訊。

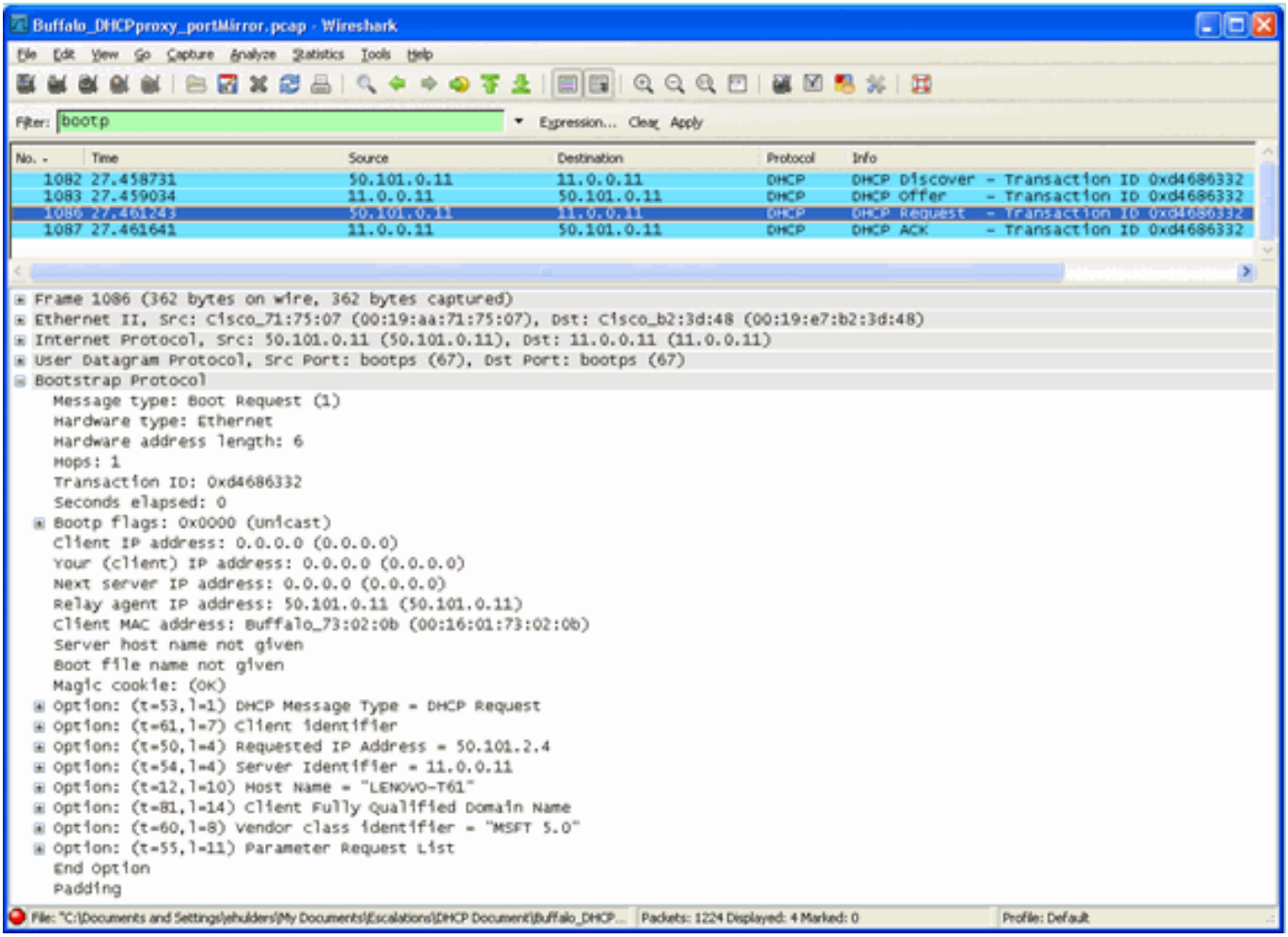
客戶端視角

此截圖是從使用者端的角度擷取的資料包擷取。其中顯示了DHCP發現、DHCP提供、DHCP請求和DHCP ACK。DHCP請求突出顯示，並且 boot p 協定詳細資訊展開，其中顯示DHCP選項。



伺服器視角

此截圖是從伺服器的角度擷取的資料包捕獲。與先前的示例類似，它顯示了DHCP發現、DHCP提供、DHCP請求和DHCP ACK。但是這些封包是控制器作為DHCP代理的函式而建立的。同樣，DHCP請求會突出顯示，並且 boot p 協定詳細資訊展開，其中顯示DHCP選項。請注意，它們與客戶端的DHCP請求資料包中的相同。另請注意，WLC代理會中繼封包並突出顯示封包位址。



代理配置示例

若要將控制器用作DHCP代理，必須在控制器上啟用DHCP代理功能。預設情況下，此功能已啟用。要啟用DHCP代理，可以使用此CLI命令。DHCP選單的Controller頁面上的GUI中也有此功能。

```
<#root>

(Cisco Controller) >

config dhcp proxy enable

(Cisco Controller) >

show dhcp proxy


DHCP Proxy Behavior: enabled
```

要使DHCP代理正常工作，必須在需要DHCP服務的每個控制器介面上配置主DHCP伺服器。可以在管理介面、ap-manager介面和動態介面上配置DHCP伺服器。可以使用這些CLI命令為每個介面配置DHCP伺服器。

```
<#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橋接功能是全域性設定，因此它會影響控制器內的所有DHCP事務。

疑難排解

這是 **debug dhcp packet enable** 指令。調試顯示一個控制器，它從MAC地址為00:40:96:b4:8c:e1的客戶端接收DHCP請求，將DHCP請求傳送到DHCP伺服器，從DHCP伺服器接收回覆，並向客戶端傳送DHCP提供。

<#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
```

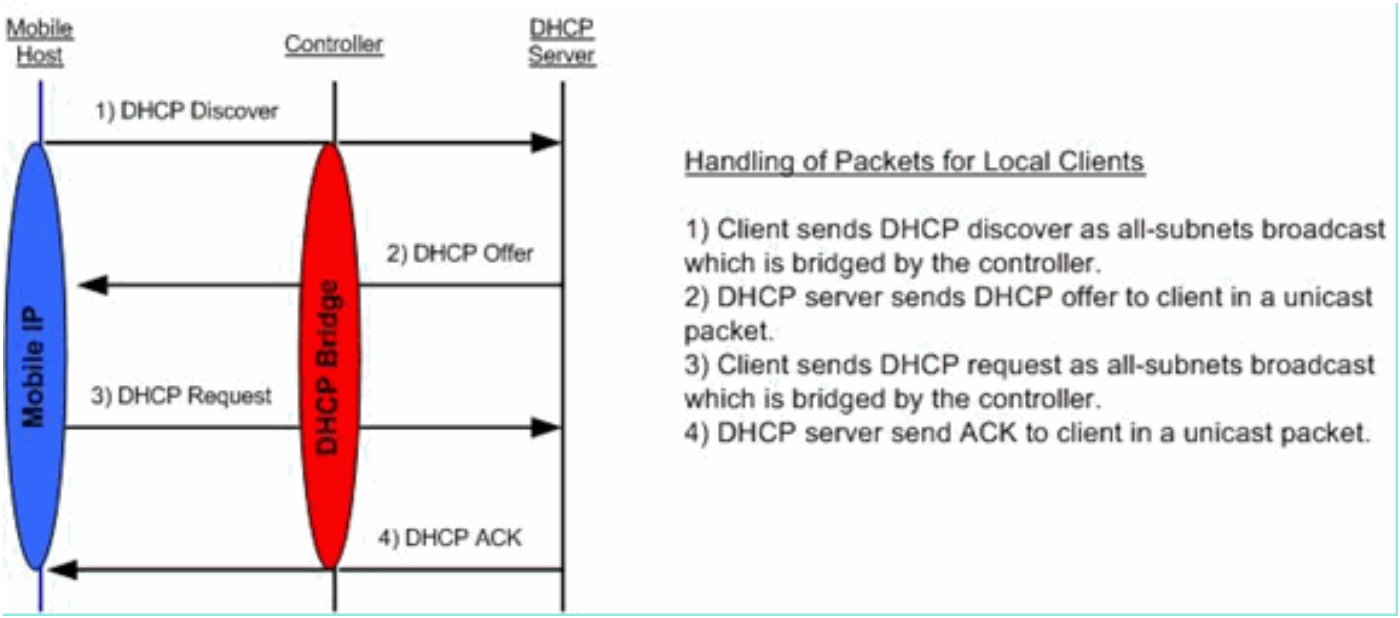
注意事項

- 啟用DHCP代理的控制器與同時充當防火牆和DHCP伺服器的裝置之間可能存在互操作性問題。這很可能是由於裝置的防火牆元件，因為防火牆通常不響應代理請求。此問題的解決方法是停用控制器上的DHCP代理。
- 當客戶端在控制器上處於DHCP REQ狀態時，控制器會丟棄DHCP通知資料包。客戶端在收到來自客戶端的DHCP發現資料包之前，不會在控制器上進入RUN狀態（這是客戶端傳遞流量所必需的）。當DHCP代理被禁用時，DHCP通知資料包由控制器轉發。
- 相互通訊的所有控制器必須具有相同的DHCP代理設定。

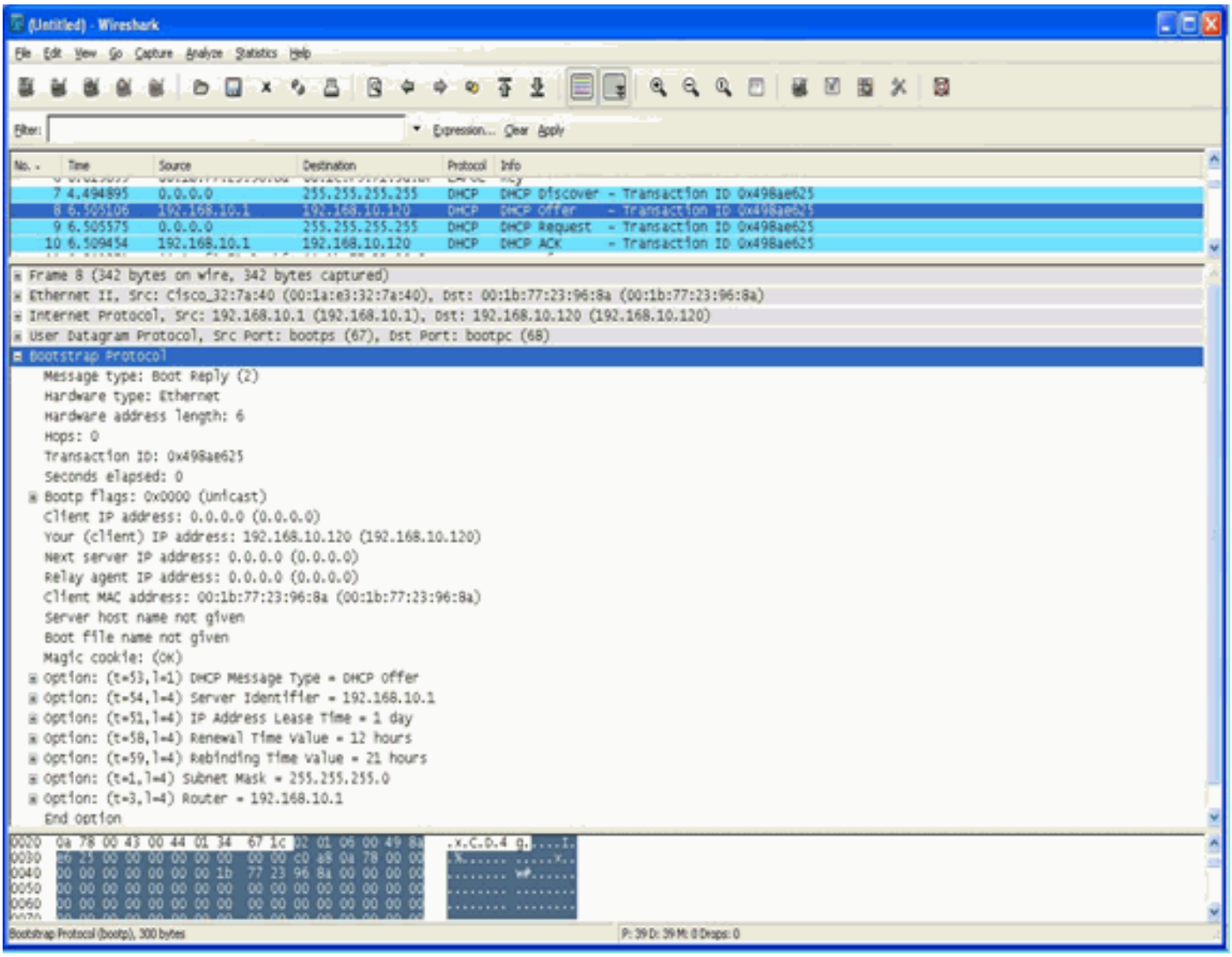
DHCP橋接模式

DHCP橋接功能旨在使DHCP事務中的控制器角色對客戶端完全透明。除802.11轉換為乙太網路II外，來自使用者端的封包不會從輕型存取點通訊協定(LWAPP)通道橋接至使用者端VLAN(或在L3漫遊情況下為Ethernet over IP(EoIP)通道)。同樣，除乙太網II到802.11轉換外，傳送到客戶端的資料包未經修改就從客戶端VLAN（或L3漫遊案例中的EoIP隧道）橋接到LWAPP隧道。將此設想為將客戶端連線到交換機埠，然後客戶端執行傳統的DHCP事務。

DHCP橋接操作 — 橋接封包流

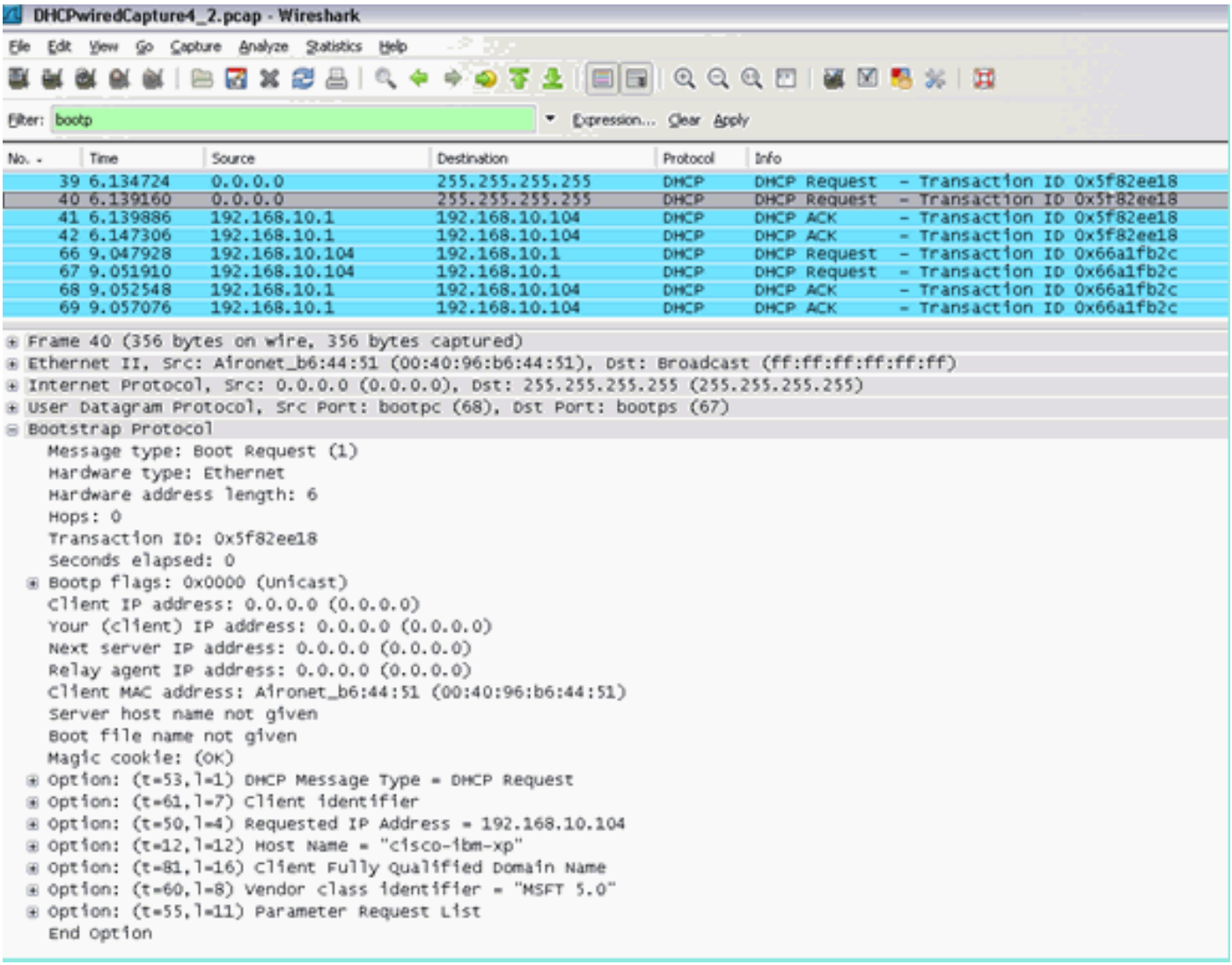


橋接封包擷取 — 使用者端視角



在客戶端資料包捕獲螢幕截圖中，代理模式下的客戶端捕獲之間的主要區別是DHCP伺服器的實際IP，即在Offer和Ack資料包中看到的實際IP，而不是控制器虛擬IP地址。

橋接封包擷取 — 伺服器透視



在有線資料包捕獲螢幕截圖中，您可以看到資料包40是從測試客戶端00:40:96:b6:44:51到有線網路的橋接DHCP請求廣播。

橋接配置示例

要在控制器上啟用DHCP橋接功能，必須在控制器上禁用DHCP代理功能。這只能在CLI中使用以下命令來完成：

<#root>

```
(Cisco Controller) >
config dhcp proxy disable
(Cisco Controller) >
show dhcp proxy
DHCP Proxy Behaviour: disabled
```

如果DHCP伺服器與客戶端不在同一第2層(L2)網路中，則必須使用IP幫助程式將廣播轉發到客戶端

網關上的DHCP伺服器。以下是此組態範例：

```
<#root>

Switch#

conf t

Switch(config)#

interface vlan




Switch(config-if)#

ip helper-address
```

DHCP橋接功能是全域性設定，因此它會影響控制器內的所有DHCP事務。您必須在有線基礎架構中為控制器上的所有必要VLAN新增IP協助程式陳述式。

疑難排解

此處列出的調試已在控制器CLI上啟用，並且輸出的DHCP部分已提取給本文檔。

```
<#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

在此DHCP偵錯輸出中，有一些重要指標表示控制器上正在使用DHCP橋接：

- DHCP成功將資料包橋接到DS — 這意味著來自客戶端的原始DHCP資料包被橋接，未更改到分佈系統(DS)。DS是有線基礎架構。
- DHCP成功將資料包橋接到STA — 此消息表示DHCP資料包已橋接，未更改到站(STA)。STA是請求DHCP的客戶端電腦。

此外，您還會看到調試中列出的實際伺服器IP地址192.168.10.1。如果正在使用DHCP代理而不是DHCP橋接，則可以看到為伺服器IP地址列出的控制器虛擬IP地址。

注意事項

- 預設情況下，DHCP代理已啟用。
- 相互通訊的所有控制器必須具有相同的DHCP代理設定。
- 必須啟用DHCP代理，DHCP選項82才能正常工作。

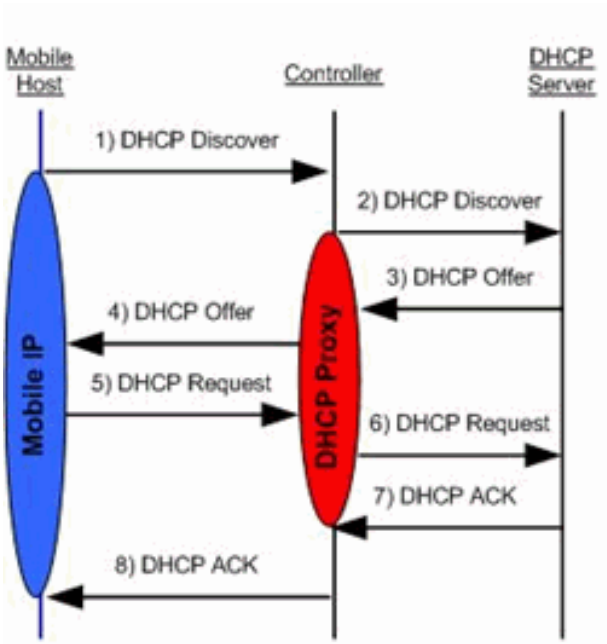
內部DHCP伺服器

內部DHCP伺服器最初是為沒有外部DHCP伺服器的分支機構引入的。它的設計目的是支援一個小型無線網路，該無線網路具有位於同一子網中的不到10個接入點(AP)。內部伺服器為無線客戶端、直接連線AP、管理介面上的裝置模式AP以及從AP中繼的DHCP請求提供IP地址。它並不是一個完整的通用DHCP伺服器。它僅支援有限的功能，並且無法在較大的部署中進行擴展。

內部DHCP和橋接模式的比較

控制器上的兩種主要DHCP模式是DHCP代理或DHCP橋接。使用DHCP橋接時，控制器的行為更像帶有自治AP的DHCP後端。DHCP資料包通過與連結到VLAN的服務集識別符號(SSID)的客戶端關聯進入AP。接著DHCP封包會離開該VLAN。如果在該VLAN的第3層(L3)網關上定義了IP幫助程式，則該資料包將通過定向單播轉發到該DHCP伺服器。然後DHCP伺服器直接對轉發該DHCP資料包的L3介面做出響應。使用DHCP代理也是同樣的想法，但所有轉發都直接在控制器上完成，而不是VLAN的第3層介面。例如，DHCP請求從客戶端進入WLAN，然後WLAN使用在VLAN介面上定義的DHCP伺服器*或*使用WLAN的DHCP覆蓋功能，將單播DHCP資料包轉發到DHCP伺服器，並填寫DHCP資料包GIADDR欄位作為VLAN介面的IP地址。

內部DHCP伺服器 — 資料包流



Handling of Packets for Local Clients

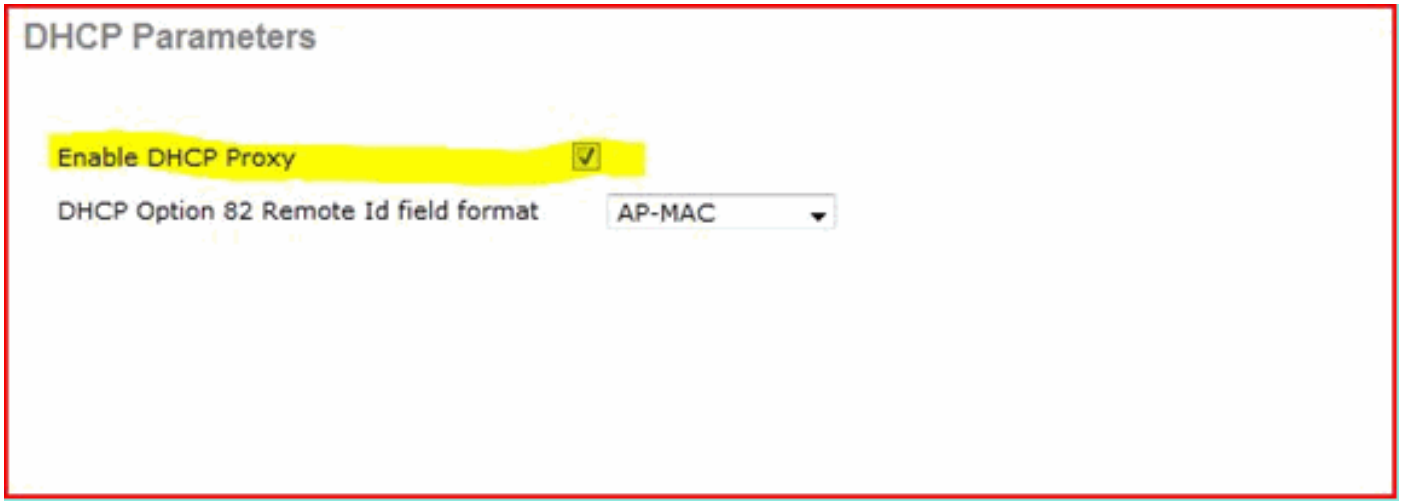
1) Client sends DHCP discover as all-subnets broadcast
2) Controller forwards the DHCP discover via the DHCP proxy service of the controller to the internal DHCP server (Note: the configured DHCP server IP address must be the management IP address of the controller).
3) Internal DHCP server sends DHCP offer back to the DHCP proxy agent on the controller.
4) Controller unicasts DHCP offer to client with option 54 and source address set as controller's management IP address.
5) Client sends DHCP request to the management IP address.
6) Controller unicasts DHCP request from WLAN IP address to DHCP proxy service which then forwards the request to the internal DHCP server.
7) Internal DHCP server sends ACK to the DHCP proxy service.
8) Controller unicasts ACK to the client.

內部DHCP伺服器配置示例

您必須在控制器上啟用DHCP代理，才能讓內部DHCP伺服器正常工作。這可透過本節下方的GUI完成：

註：您不能在所有版本中通過GUI設定DHCP代理。

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

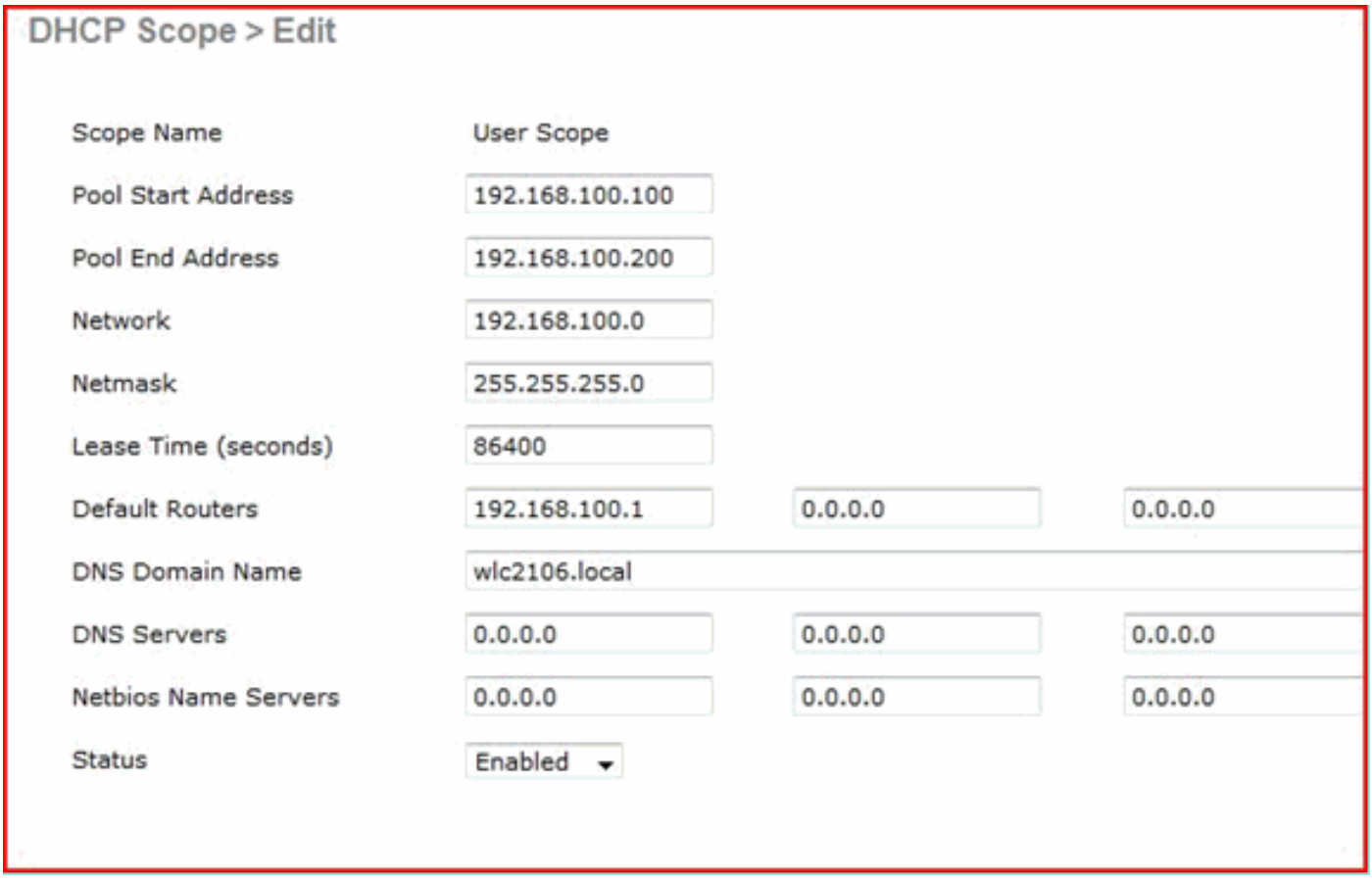


或透過CLI:

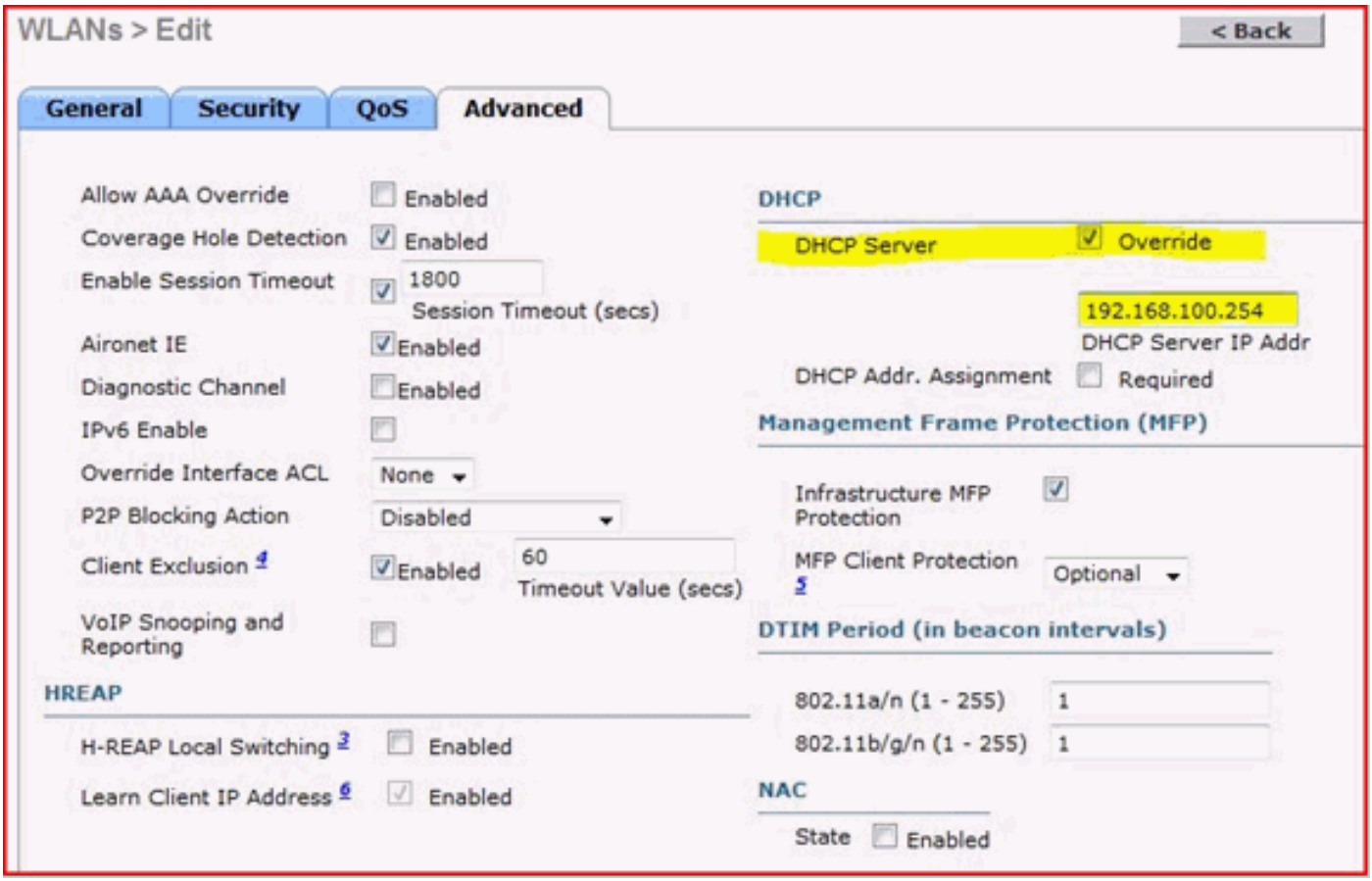
```
Config dhcp proxy enable
Save config
```

要啟用內部DHCP伺服器，請完成以下步驟：

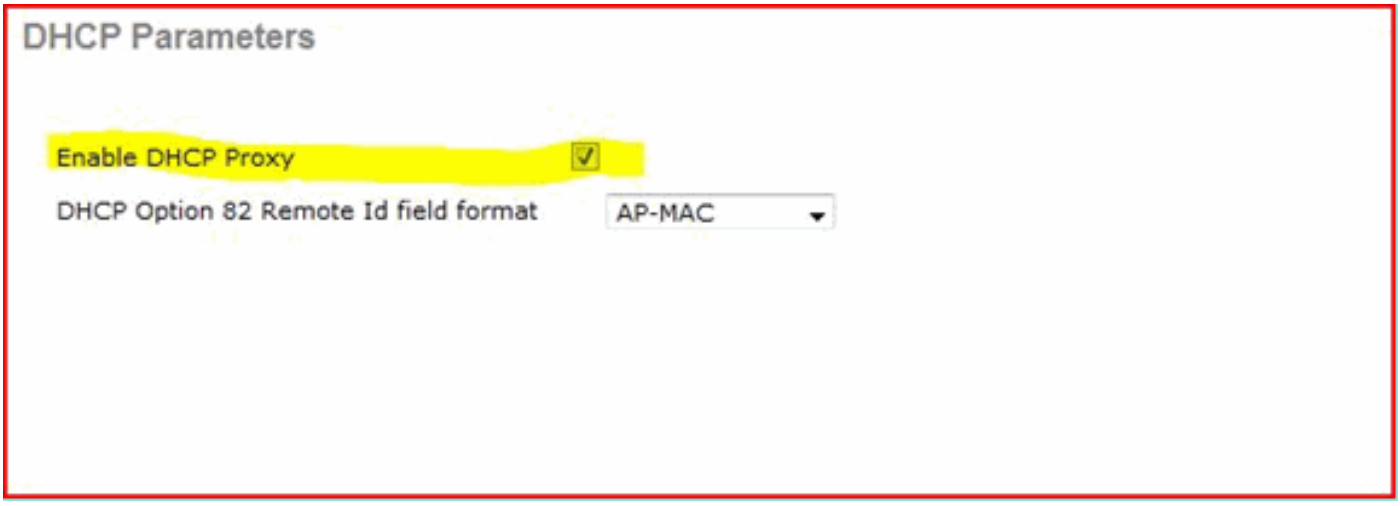
1.定義用於提取IP地址的作用域(Controller > Internal DHCP Server > DHCP Scope)。按一下 New.



2.將DHCP覆蓋指向控制器的管理介面IP地址。



3.確保DHCP代理已啟用。



疑難排解

內部DHCP伺服器的調試通常要求查詢在獲取IP地址時遇到問題的客戶端。您必須運行這些debug。

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

debug client是一個宏，它為您啟用這些調試，同時它只將調試集中在您輸入的客戶端MAC地址上。

```
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問題的主要問題是 debug dhcp packet enable 命令自動啟用 debug client 指令。

<#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
```

清除WLC內部DHCP伺服器上的DHCP租用

您可以發出以下命令，清除WLC的內部DHCP伺服器上的DHCP租用：

```
<#root>

config dhcp clear-lease
```

以下是範例：

```
<#root>

config dhcp clear-lease all
```

注意事項

- 必須啟用DHCP代理，內部DHCP伺服器才能正常工作
- 使用受CPU ACL影響的內部DHCP伺服器時，使用DHCP連線到埠1067
- 內部DHCP伺服器通過127.0.0.1 UDP埠67監聽控制器環回介面

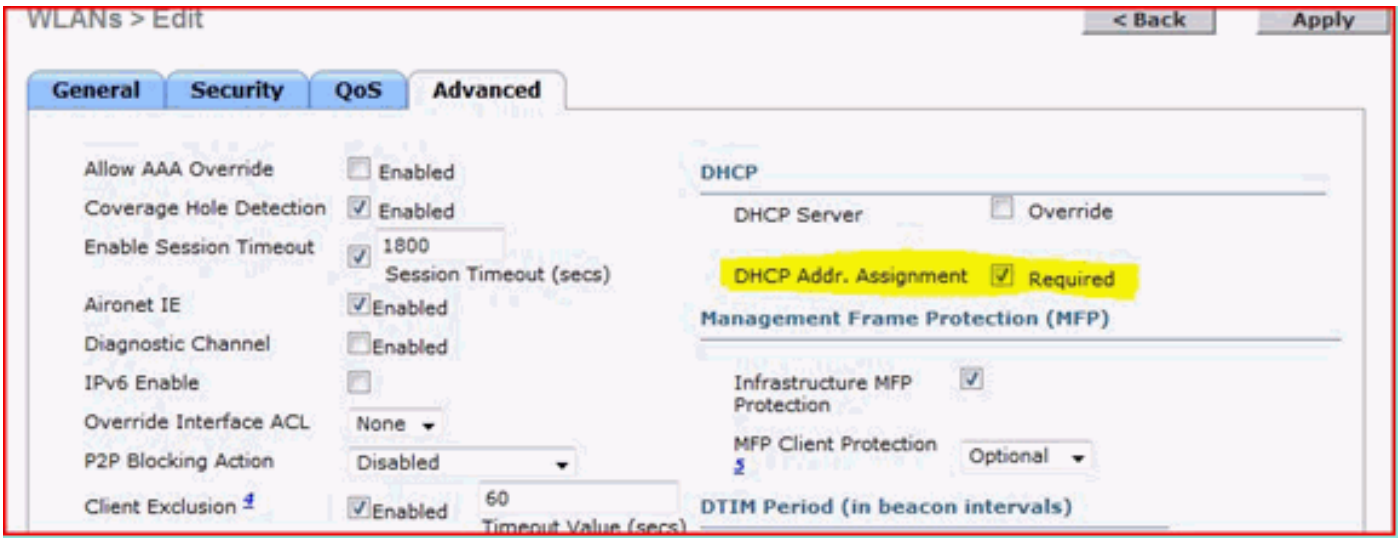
終端使用者介面

- 其 **config dhcp proxy disable** 命令表示使用DHCP橋接功能。這是一個全域命令（不是每個WLAN的命令）。

- 預設情況下，DHCP代理保持啟用狀態。
- 禁用DHCP代理後，本地WLAN將無法使用內部DHCP伺服器。橋接操作與將資料包重定向到內部伺服器所需的操作不一致。橋接確實意味著橋接，但802.11到乙太網II的轉換除外。DHCP封包會以未修改的方式從LWAPP通道傳遞到使用者端VLAN（反之亦然）。
- 啟用代理後，必須在WLAN的介面（或WLAN本身）上設定DHCP伺服器，才能啟用WLAN。禁用代理時，無需配置任何伺服器，因為這些伺服器未使用。
- 當使用者嘗試啟用DHCP代理時，可以在內部驗證所有WLAN（或關聯介面）是否配置了DHCP伺服器。否則，啟用操作失敗。

需要DHCP

WLAN進階組態有一個選項，要求使用者在進入RUN狀態（使用者端可以透過控制器傳輸流量的狀態）之前傳遞DHCP。此選項要求客戶端執行完整或半個DHCP請求。控制器從客戶端查詢的主要內容是DHCP請求和從DHCP伺服器返回的ACK。只要客戶端執行這些步驟，客戶端就會通過DHCP必需步驟並進入RUN狀態。



L2和L3漫遊

L2 Roam - 如果使用者端具有有效的DHCP租用，並在同一L2網路上的兩個不同控制器之間執行L2漫遊，則使用者端必須不需要重新執行DHCP，而且使用者端專案必須完全從原始控制器移動到新控制器。接下來，如果使用者端需要再次使用DHCP，則目前控制器上的DHCP橋接或代理程式會透明地再次橋接封包。

L3 Roam - 在L3漫遊情況下，客戶端會在不同L3網路的兩個不同控制器之間移動。在這種情況下，客戶端將錨定到原始控制器並在新的外部控制器上的客戶端表中列出。在錨點場景中，當客戶端資料在外部控制器和錨點控制器之間的EoIP隧道內進行隧道傳輸時，錨點控制器會處理客戶端DHCP。

相關資訊

- 輕量型 Cisco Aironet 存取點的 DHCP 選項 43 組態範例
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。