了解AireOS WLC如何处理DHCP协议

目录

简介

本文档介绍Cisco AireOS无线控制器上的不同DHCP操作。

外部 DHCP 服务器

在使用外部DHCP服务器的情况下，无线LAN控制器(WLC)支持两种DHCP操作模式：

- DHCP 代理模式
- DHCP 桥接模式

DHCP代理模式用作DHCP帮助功能，以便在DHCP服务器和无线客户端之间实现更好的安全性和对DHCP事务的控制。DHCP桥接模式提供了使控制器角色在DHCP事务中对无线客户端完全透明的选项。

DHCP 代理和桥接模式比较

处理客户端 DHCP	DHCP 代理模式	DHCP 桥接模式
修改 giaddr	Yes	无
修改 siaddr	Yes	无
修改数据包内容	Yes	无
不转发冗余内容	Yes	无
选项 82 支持	Yes	无
广播到单播	Yes	无
BOOTP 支持	无	服务器
不符合 RFC	代理和中继代理的概念不完全相同。推荐使用 DHCP 桥接模式，这样才能完全符合 RFC 标准。	无

DHCP 代理模式

DHCP 代理并不适用于所有网络环境。控制器修改并中继所有DHCP事务，以提供帮助功能并解决某些安全问题。

控制器虚拟IP地址通常用作客户端的所有DHCP事务的源IP地址。因此，不会公开真实的 DHCP 服务器 IP 地址。此虚拟 IP 在控制器上的 DHCP 事务的 debug 输出中显示。但是，使用虚拟IP地址可能会导致某些类型的客户端出现问题。

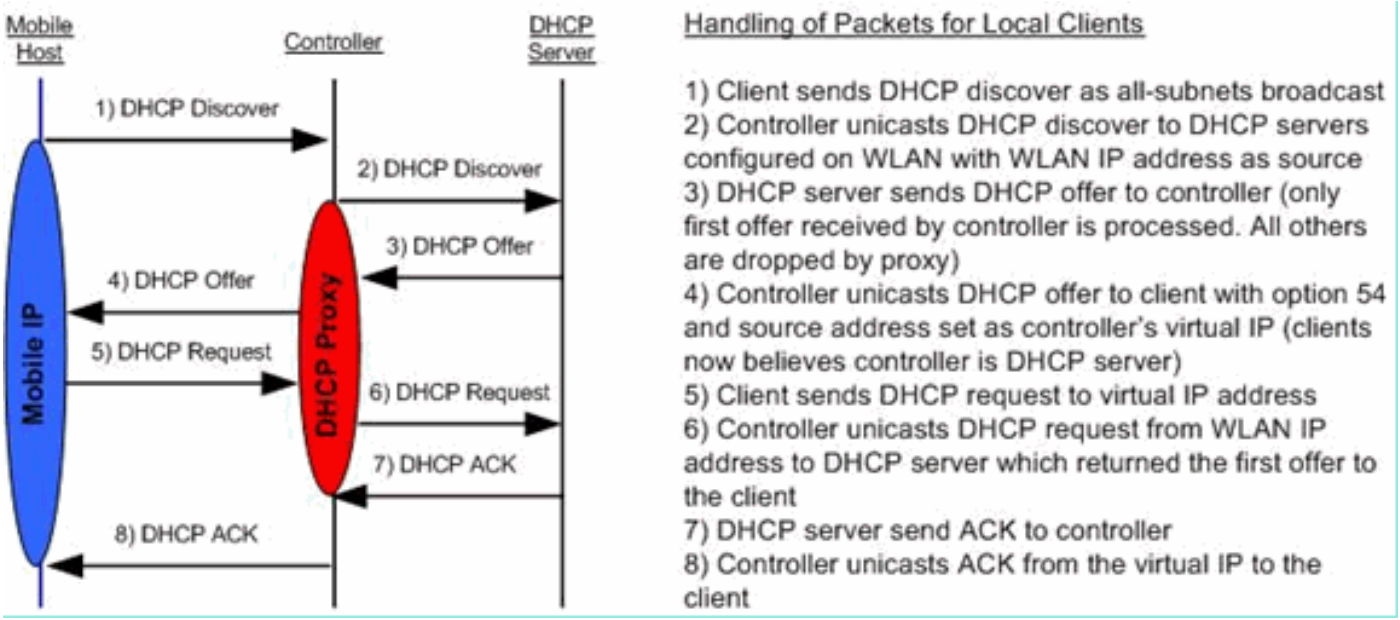
对于对称和非对称移动协议，DHCP代理模式操作保持相同的行为。

当来自外部DHCP服务器的多个提供时，DHCP代理通常会选择第一个提供并在客户端数据结构中设置服务器的IP地址。因此，所有后续事务都通过同一DHCP服务器运行，直到事务在重试后失败。这时，代理将为客户端选择其他 DHCP 服务器。

默认情况下会启用 DHCP 代理。所有进行通信的控制器都必须具有相同的DHCP代理设置。

注：必须启用DHCP代理，DHCP选项82才能正常运行。

代理数据包流

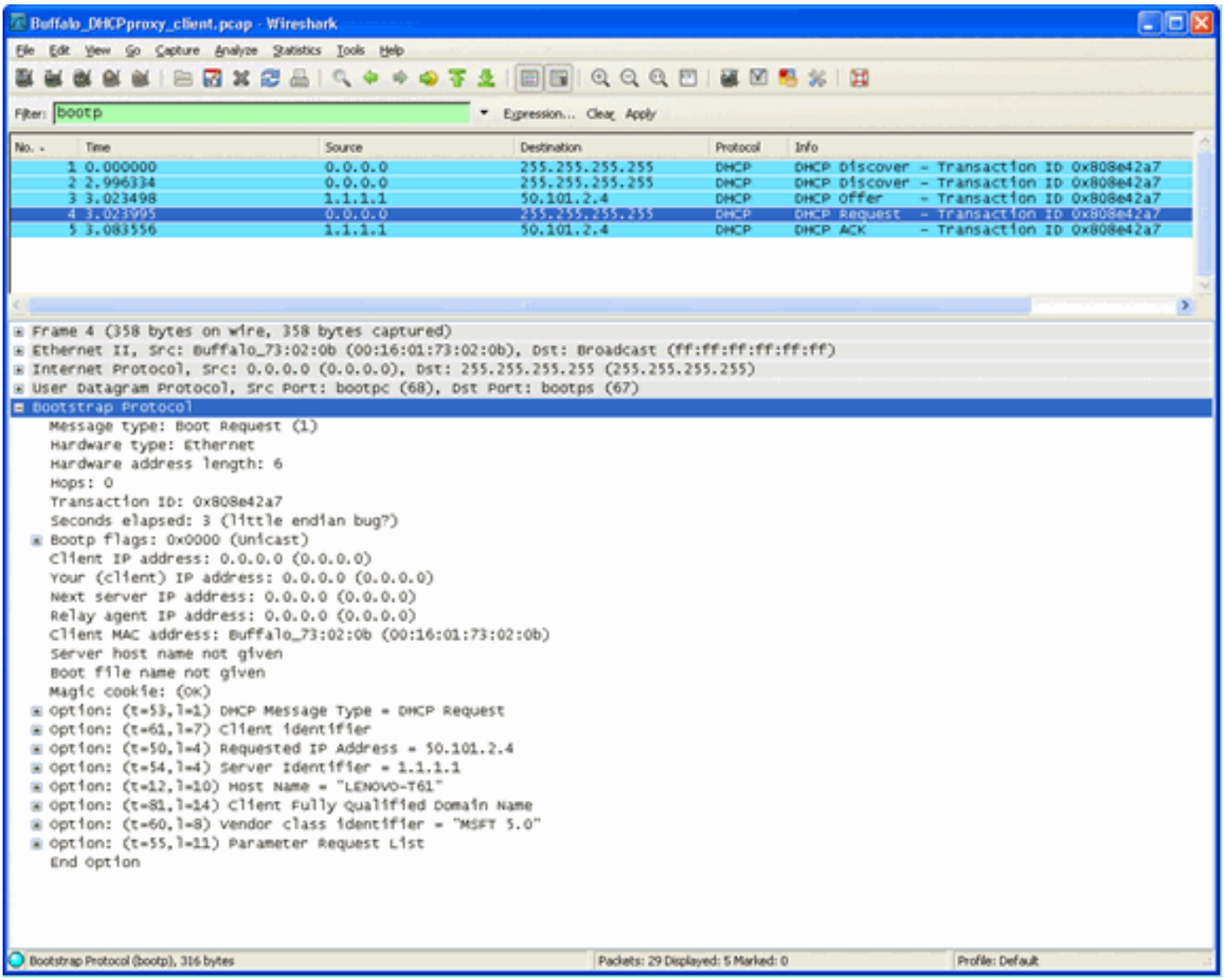


代理数据包捕获

当控制器处于DHCP代理模式时，它不仅会将DHCP数据包定向到DHCP服务器，还会实际构建新的DHCP数据包以转发到DHCP服务器。客户端DHCP数据包中存在的所有DHCP选项均复制到控制器DHCP数据包中。接下来的屏幕截图示例显示了 DHCP 请求数据包的这一过程。

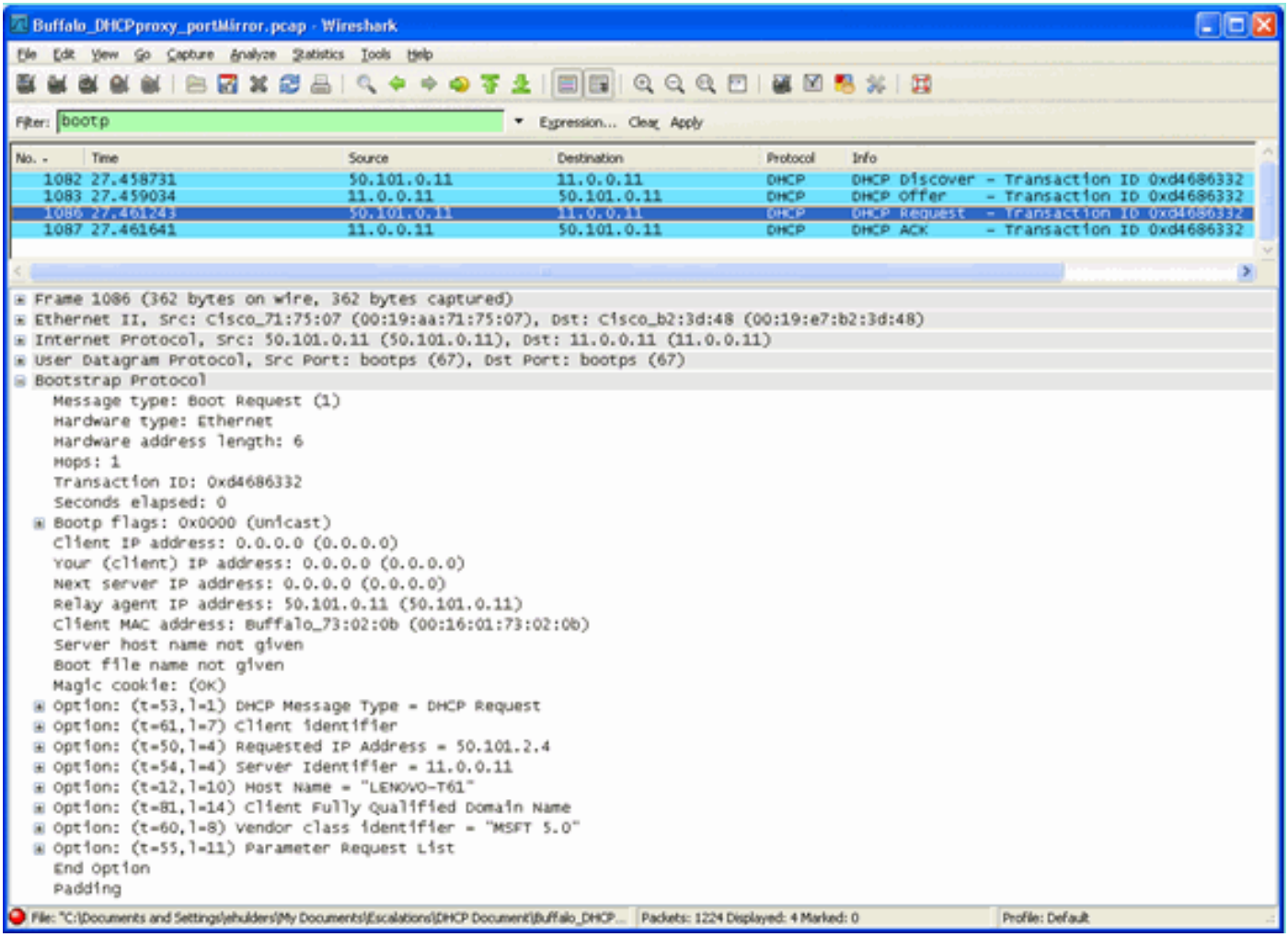
客户端角度

此屏幕截图是从客户端角度捕获的数据包信息。它显示了 DHCP 发现，DHCP 提供、DHCP 请求和 DHCP ACK。DHCP请求突出显示，并且 boot p 协议详细信息已展开，其中显示了DHCP选项。



服务器角度

此屏幕截图是从服务器的角度捕获的数据包信息。类似于前一示例，它显示了 DHCP 发现，DHCP 提供、DHCP 请求和 DHCP ACK。但是，这些数据包是控制器作为DHCP代理的功能构建的。同样，DHCP请求会突出显示，并且 boot p 协议详细信息已展开，其中显示了DHCP选项。请注意，它们与客户端的DHCP请求数据包中的相同。另请注意，WLC代理会中继数据包并突出显示数据包地址。



代理配置示例

要将控制器用作DHCP代理，必须在控制器上启用DHCP代理功能。默认情况下会启用此功能。要启用DHCP代理，可以使用此CLI命令。DHCP菜单中的Controller页面上的GUI中也会显示相同的内容。

<#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，必须在需要DHCP服务的每个控制器接口上配置主DHCP服务器。DHCP服务器可以在管理接口、ap-manager接口和动态接口上配置。可以使用这些CLI命令为每个接口配置DHCP服务器。

<#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 桥接功能是一项全局设置，因此会影响控制器内的所有 DHCP 事务。

故障排除

这是 **debug dhcp packet enable** 命令。调试显示了一个控制器，该控制器接收来自MAC地址为00:40:96:b4:8c:e1的客户端的DHCP请求，向DHCP服务器发送DHCP请求，从DHCP服务器接收应答，并向客户端发送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
```

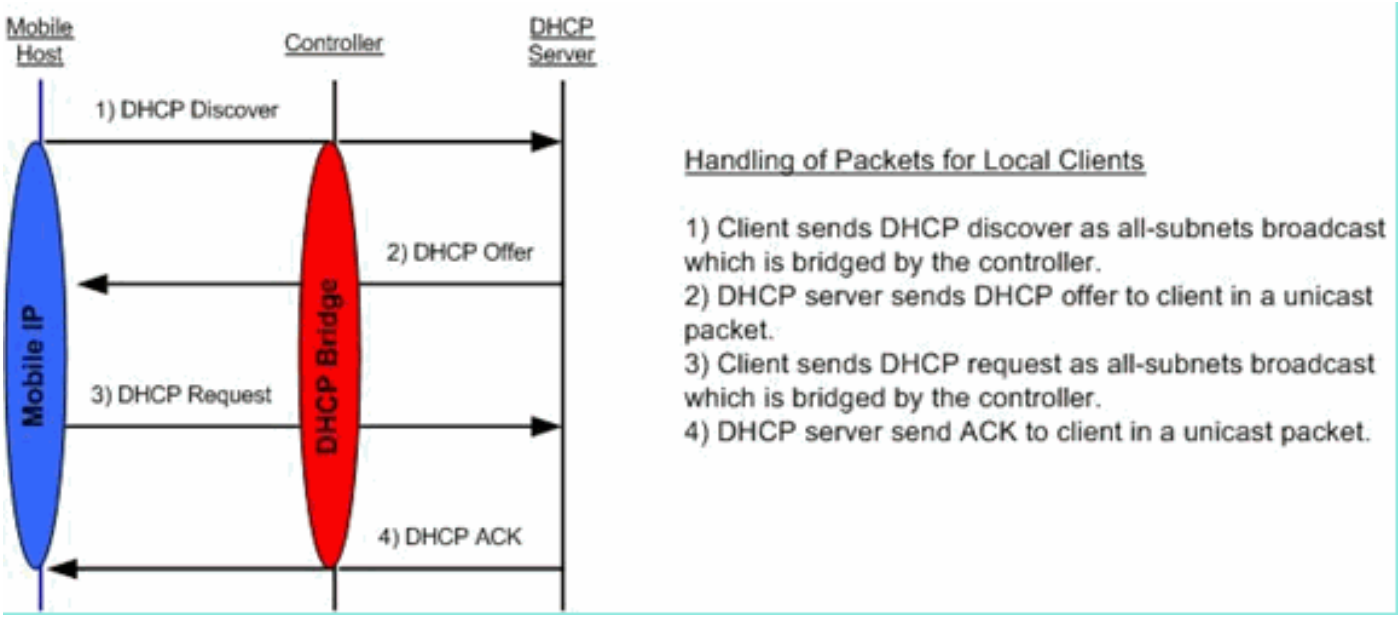
注意事项

- 启用DHCP代理的控制器与同时充当防火墙和DHCP服务器的设备之间可能存在互操作性问题。通常情况下，这很可能是由于设备的防火墙组件作为防火墙无法响应代理请求引起的。此问题的解决方法是禁用控制器上的DHCP代理。
- 当客户端在控制器上处于DHCP REQ状态时，控制器会丢弃DHCP通知数据包。客户端在收到来自客户端的DHCP发现数据包之前，不会在控制器上进入RUN状态（这是客户端传递流量所必需的）。当DHCP代理被禁用时，控制器会转发DHCP通知数据包。
- 相互通信的所有控制器必须具有相同的DHCP代理设置。

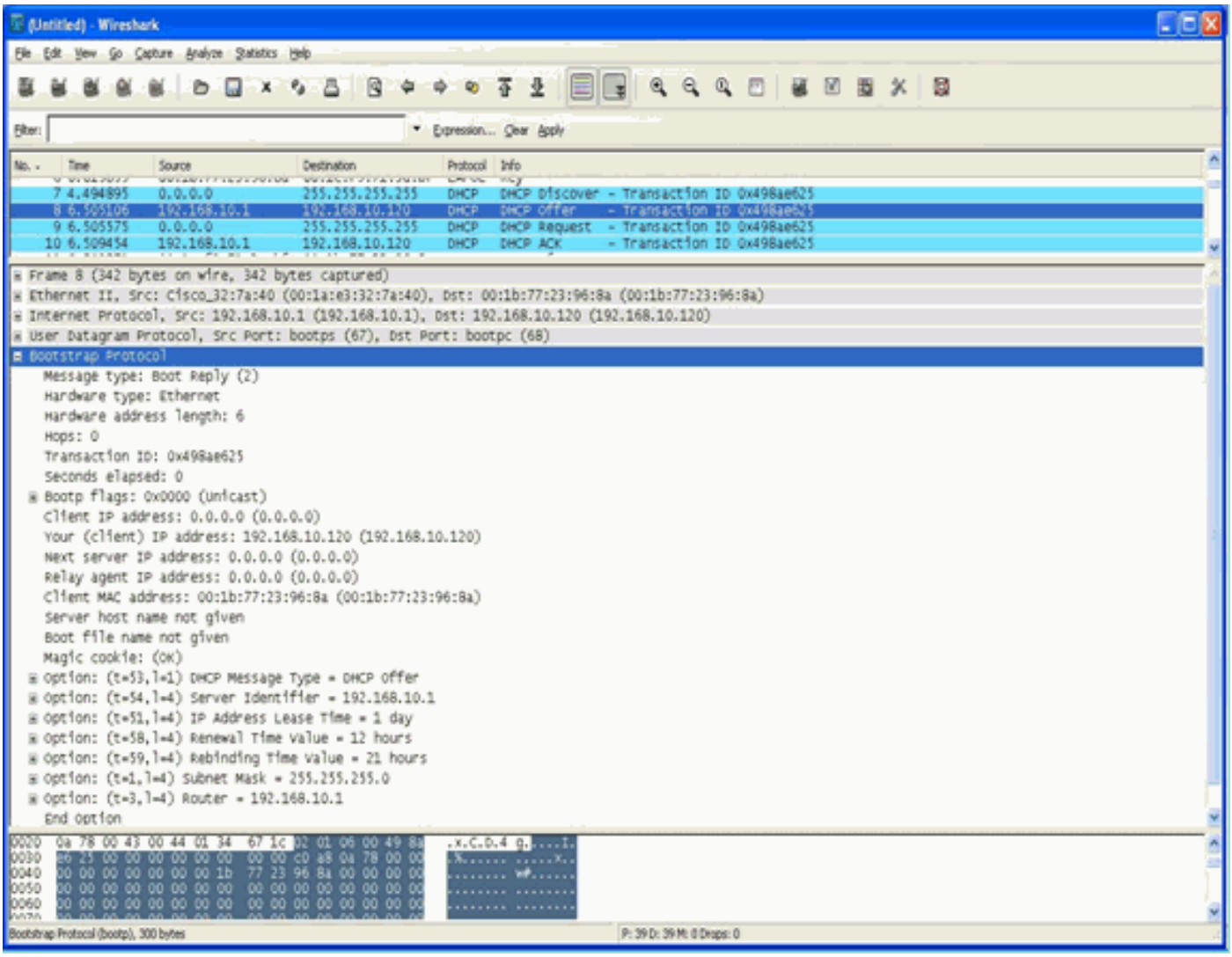
DHCP 桥接模式

DHCP桥接功能旨在使DHCP事务中的控制器角色对客户端完全透明。除802.11到以太网II的转换外，来自客户端的数据包未经修改从轻量接入点协议(LWAPP)隧道桥接到客户端VLAN(或L3漫游情况下的基于IP的以太网(EoIP)隧道)。同样，除了以太网II到802.11的转换之外，发送到客户端的数据包未经修改从客户端VLAN（或L3漫游案例中的EoIP隧道）桥接到LWAPP隧道。将此设想为将客户端连接到交换机端口，然后客户端执行传统的DHCP事务。

DHCP 桥接操作 - 桥接数据包流

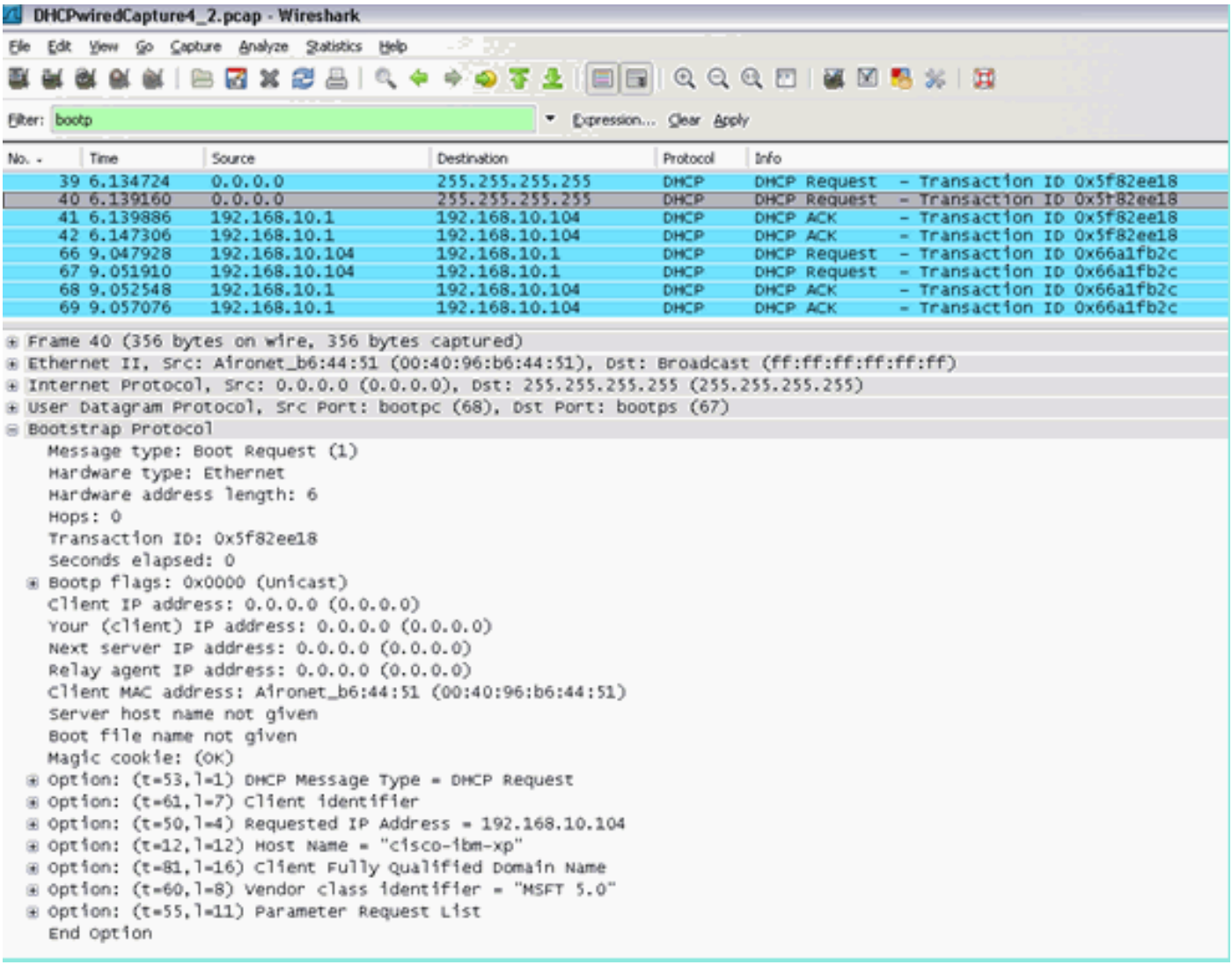


桥接数据包捕获 - 客户端角度



在客户端数据包捕获屏幕截图中，代理模式下的客户端捕获之间的主要区别是DHCP服务器的实际IP，在Offer和Ack数据包中看到的不是控制器虚拟IP地址。

桥接数据包捕获 - 服务器角度



在有线数据包捕获屏幕截图中，您可以看到数据包40是从测试客户端00:40:96:b6:44:51到有线网络的桥接DHCP请求广播。

桥接配置示例

要在控制器上启用DHCP桥接功能，必须在控制器上禁用DHCP代理功能。这只能在CLI中使用以下命令来完成：

```
<#root>

(Cisco Controller) >

config dhcp proxy disable

(Cisco Controller) >

show dhcp proxy

DHCP Proxy Behaviour: disabled
```

如果DHCP服务器与客户端不在同一第2层(L2)网络中，则必须使用IP帮助程序将广播转发到客户端

网关处的DHCP服务器。以下是此配置的一个示例：

```
<#root>

Switch#

conf t

Switch(config)#

interface vlan




Switch(config-if)#

ip helper-address
```

DHCP 桥接功能是一项全局设置，因此会影响控制器内的所有 DHCP 事务。必须在有线基础架构中为控制器上的所有必要VLAN添加IP帮助语句。

故障排除

此处列出的 debug 已在控制器 CLI 上启用，并且已针对本文档提取出了输出的 DHCP 部分。

```
<#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 debug 输出中，有一些表明控制器正使用 DHCP 桥接的重要指示：

- DHCP成功将数据包桥接到DS — 这意味着来自客户端的原始DHCP数据包被桥接到，未更改到分布系统(DS)。DS 为有线基础架构。
- DHCP成功将数据包桥接到STA — 此消息表明DHCP数据包已桥接且未更改到站点(STA)。STA是请求DHCP的客户端。

此外，您还会看到调试中列出的实际服务器IP地址，即192.168.10.1。如果正在使用DHCP代理而不是DHCP桥接，您可以看到为服务器IP地址列出的控制器虚拟IP地址。

注意事项

- 默认情况下，DHCP代理已启用。
- 相互通信的所有控制器必须具有相同的DHCP代理设置。
- 要使 DHCP 选项 82 工作，必须启用 DHCP 代理。

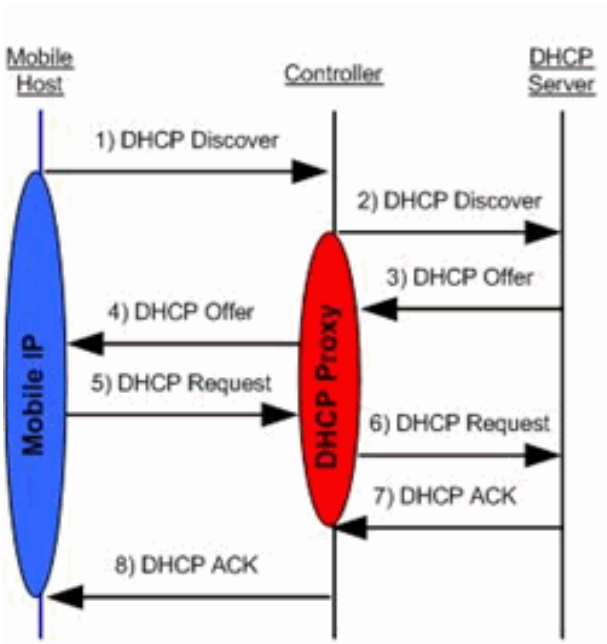
内部 DHCP 服务器

内部 DHCP 服务器最初是为无法使用外部 DHCP 服务器的分支机构引入的。它旨在支持小型无线网络，同一子网中的接入点(AP)少于十个。内部服务器向管理接口上的无线客户端、直连 AP、设备模式 AP 提供 IP 地址，以及从 AP 转发的 DHCP 请求。它不是成熟的通用DHCP服务器。它仅支持有限的功能，在大型部署中无法扩展。

内部 DHCP 和桥接模式比较

控制器上的两种主要 DHCP 模式为 DHCP 代理或 DHCP 桥接。使用DHCP桥接时，控制器更像使用自治AP的DHCP回传。DHCP数据包通过与链接到VLAN的服务集标识符(SSID)的客户端关联进入AP。然后，DHCP 数据包会离开该 VLAN。如果在该VLAN的第3层(L3)网关上定义了IP帮助程序，则数据包将通过定向单播转发到该DHCP服务器。然后，DHCP服务器直接回复转发该DHCP数据包的L3接口。使用DHCP代理也是同样的想法，但所有转发都直接在控制器上完成，而不是VLAN的L3接口。例如，DHCP请求从客户端进入WLAN，然后WLAN使用VLAN接口上定义的DHCP服务器*或*使用WLAN的DHCP覆盖功能，以便将单播DHCP数据包转发到DHCP服务器，DHCP数据包GIADDR字段已填写为VLAN接口的IP地址。

内部 DHCP 服务器 - 数据包流



Handling of Packets for Local Clients

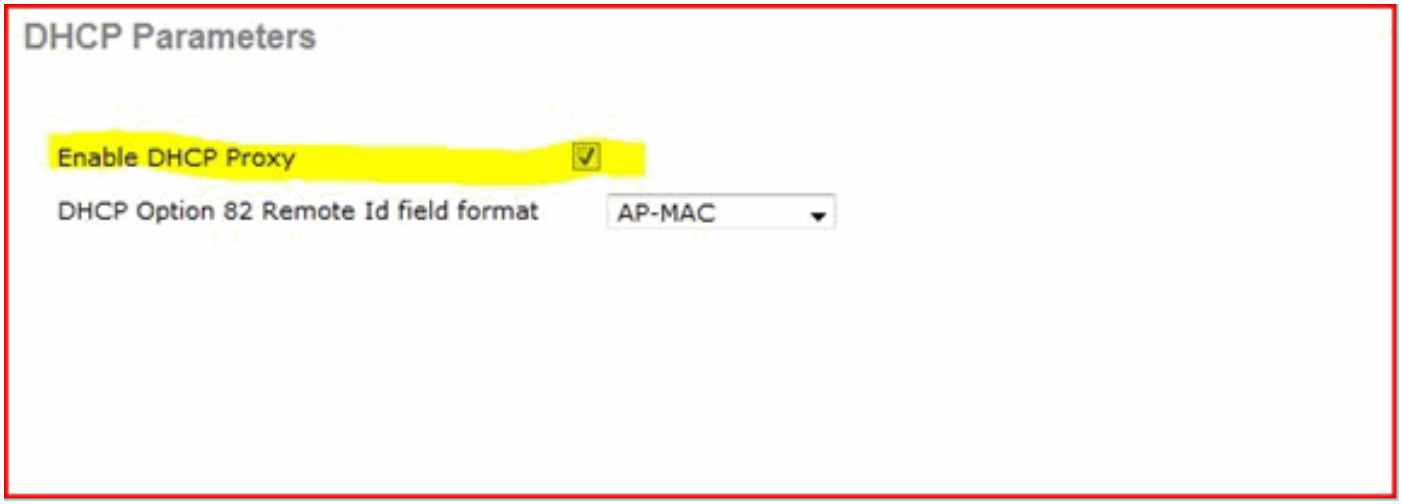
1) Client sends DHCP discover as all-subnets broadcast
2) Controller forwards the DHCP discover via the DHCP proxy service of the controller to the internal DHCP server (Note: the configured DHCP server IP address must be the management IP address of the controller).
3) Internal DHCP server sends DHCP 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.

内部 DHCP 服务器配置示例

必须在控制器上启用DHCP代理，以使内部DHCP服务器正常工作。可以通过以下 GUI 启用 DHCP 代理：

注：您不能在所有版本中通过GUI设置DHCP代理。

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

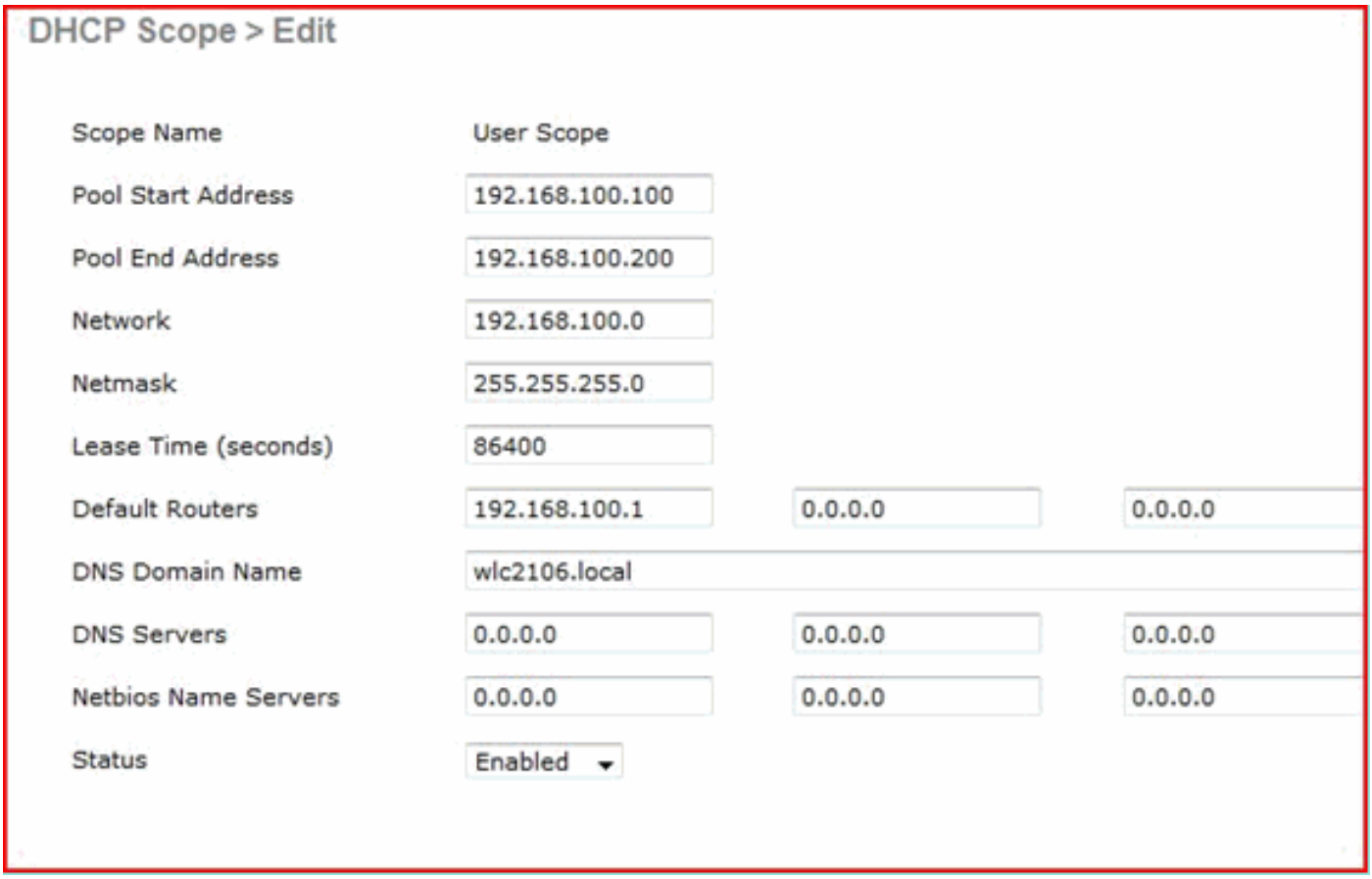


也可通过 CLI 启用 DHCP 代理：

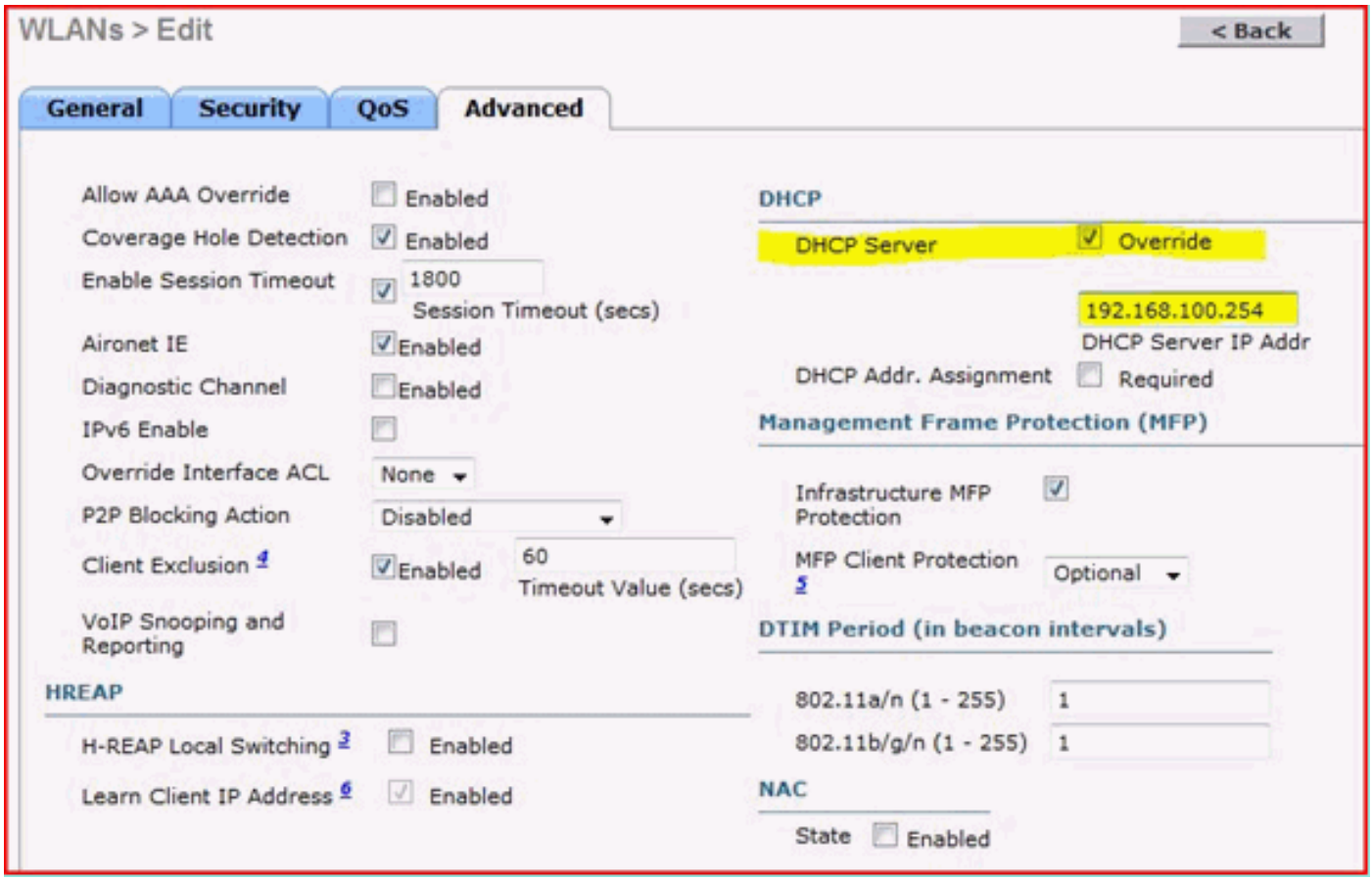
```
Config dhcp proxy enable
Save config
```

要启用内部DHCP服务器，请完成以下步骤：

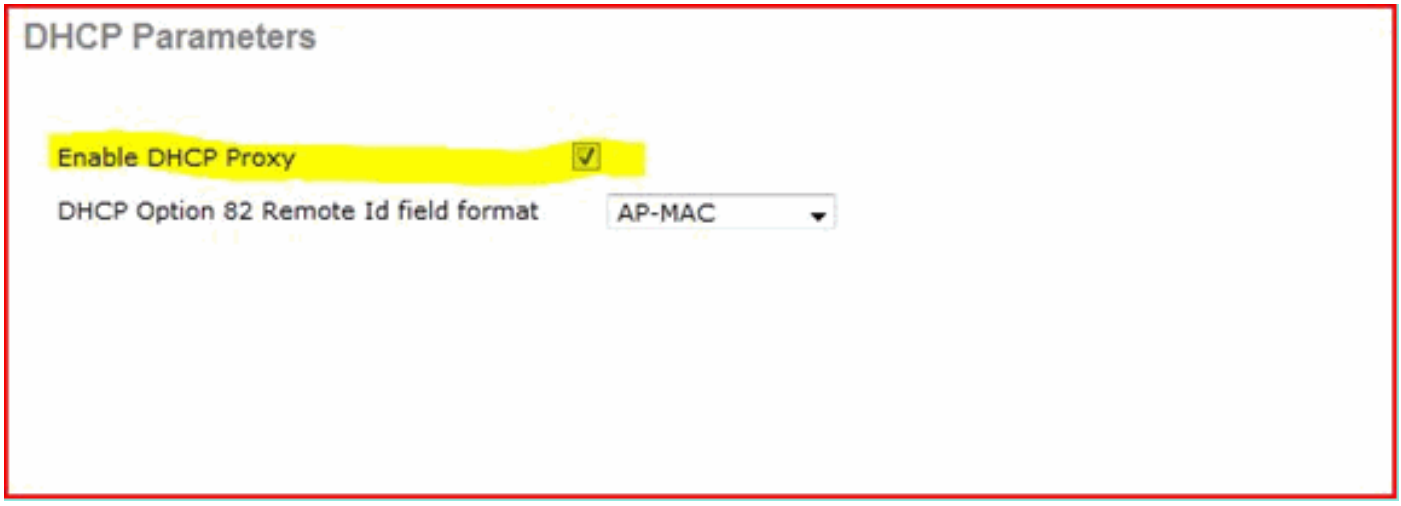
1.定义用于提取IP地址(Controller > Internal DHCP Server > DHCP Scope影响。点击 New.



2.将DHCP覆盖指向控制器的管理接口IP地址。



3.确保DHCP代理已启用。



故障排除

内部DHCP服务器的调试通常需要查找在获取IP地址时遇到问题的客户端。您必须运行这些调试。

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

debug client是一个宏，它只将调试集中在您输入的客户端MAC地址上，并为您启用这些调试。

```
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问题的主要原因是 debug dhcp packet enable 命令自动启用 debug client 命令。

<#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内部DHCP服务器上的DHCP租用

您可以发出以下命令以清除WLC的内部DHCP服务器上的DHCP租用：

<#root>

config dhcp clear-lease

例如：

<#root>

config dhcp clear-lease all

注意事项

- 必须启用DHCP代理，内部DHCP服务器才能正常工作
- 使用受CPU ACL影响的内部DHCP服务器时，对端口1067使用DHCP
- 内部DHCP服务器通过127.0.0.1 UDP端口67侦听控制器环回接口

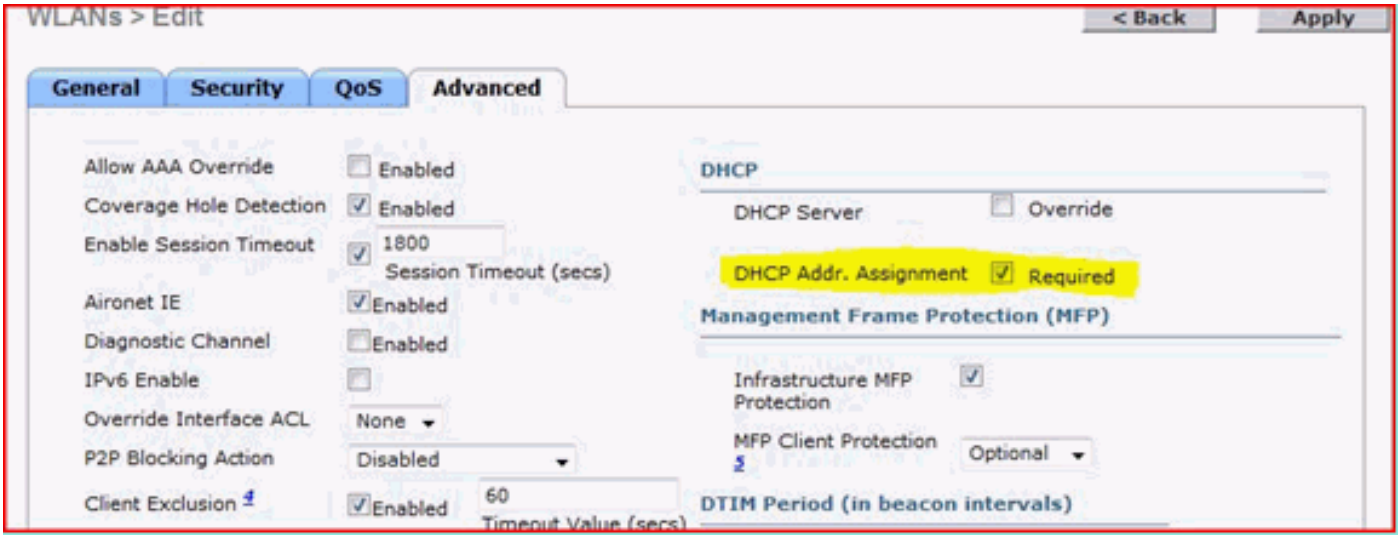
最终用户接口

- 此 **config dhcp proxy disable** 命令表示使用DHCP桥接功能。这是一个全局命令（不是基于 WLAN 的命令）。
- 默认情况下，DHCP代理保持启用状态。

- 禁用 DHCP 代理时，本地 WLAN 将无法使用内部 DHCP 服务器。桥接操作不同于将数据包重定向到内部服务器所需的操作。桥接实际上意味着桥接，但802.11到以太网II的转换除外。DHCP数据包未经修改即从LWAPP隧道传递到客户端VLAN（反之亦然）。
- 启用代理时，必须在 WLAN 的接口上（或直接在 WLAN 中）配置 DHCP 服务器，以便启用 WLAN。禁用代理时，将不需要配置服务器，因为将不会使用这些服务器。
- 用户尝试启用 DHCP 代理时，应在内部确保所有 WLAN（或关联的接口）均已配置 DHCP 服务器。否则，启用操作会失败。

所需的 DHCP

WLAN高级配置有一个选项，要求用户在进入RUN状态（客户端可以通过控制器传输流量的状态）之前通过DHCP。此选项要求客户端执行整个或半个 DHCP 请求。控制器从客户端查找的主要内容是DHCP请求和从DHCP服务器返回的ACK。只要客户端执行这些步骤，客户端就会通过DHCP所需步骤并进入RUN状态。



L2 和 L3 漫游

L2漫游 — 如果客户端具有有效的DHCP租用，并在同一L2网络上的两个不同控制器之间执行L2漫游，则客户端无需重新配置DHCP，并且客户端条目必须完全从原始控制器移动到新控制器。然后，如果客户端需要再执行DHCP，则当前控制器上的DHCP桥接或代理进程会再次透明地桥接数据包。

L3漫游 — 在L3漫游场景中，客户端在不同L3网络中的两个不同控制器之间移动。在这种情况下，客户端将锚定到原始控制器并在新的外部控制器的客户端表中列出。在锚点场景中，当客户端数据在外部控制器和锚点控制器之间的EoIP隧道内进行隧道传输时，锚点控制器会处理客户端DHCP。

相关信息

- 轻量 Cisco Aironet 接入点配置的 DHCP OPTION 43 示例

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。