

WLC与DHCP

目录

[简介](#)

[外部 DHCP 服务器](#)

[DHCP 代理和桥接模式比较](#)

[DHCP 代理模式](#)

[代理数据包流](#)

[代理数据包捕获](#)

[代理配置示例](#)

[故障排除](#)

[警告](#)

[DHCP 桥接模式](#)

[DHCP 桥接操作 - 桥接数据包流](#)

[桥接数据包捕获 - 客户端角度](#)

[桥接数据包捕获 - 服务器角度](#)

[桥接配置示例](#)

[故障排除](#)

[警告](#)

[内部 DHCP 服务器](#)

[内部 DHCP 和桥接模式比较](#)

[内部 DHCP 服务器 - 数据包流](#)

[内部 DHCP 服务器配置示例](#)

[故障排除](#)

[清除在WLC's内部DHCP服务器的DHCP租约](#)

[警告](#)

[最终用户接口](#)

[所需的 DHCP](#)

[L2 和 L3 漫游](#)

[相关信息](#)

简介

本文描述在无线控制器的不同的DHCP操作，提供一致和准确的信息给管理员查找排除故障他们的网络。

外部 DHCP 服务器

无线局域网控制器(WLC)支持DHCP操作两个模式，万一使用一个外部DHCP服务器：

- DHCP 代理模式
- DHCP 桥接模式

DHCP代理模式担当DHCP辅助功能为了达到更加好的安全和控制对DHCP处理在DHCP服务器和无

线客户端之间。DHCP桥接模式提供一个选项使在DHCP处理的控制器的作用完全地透明对无线客户端。

DHCP 代理和桥接模式比较

| 处理客户端 DHCP | DHCP 代理模式 | DHCP 桥模式 |
|------------|--|----------|
| 修改 giaddr | 是 | 否 |
| 修改 siaddr | 是 | 否 |
| 修改数据包内容 | 是 | 否 |
| 不转发冗余内容 | 是 | 否 |
| 选项82支持 | 是 | 否 |
| 对单播的广播 | 是 | 否 |
| BOOTP 支持 | 否 | 服务器 |
| 固执的RFC | 代理和中继代理不完全是同一个概念。推荐使用 DHCP 桥接模式，这样才能完全符合 RFC 标准。 | 否 |

DHCP 代理模式

DHCP 代理并不适用于所有网络环境。控制器修改并且中继所有DHCP处理提供辅助功能和解决某些安全问题。

控制器的虚拟 IP 地址通常作为所有 DHCP 事务向客户端通信的源 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。然而，使用一个虚拟IP地址能导致在客户端特定类型的问题。

不管是对称移动协议还是非对称移动协议，DHCP 代理模式操作的行为都是相同的。

当多次提供来自外部DHCP服务器时，DHCP代理通常选择进来并且设置服务器的IP地址在客户端数据数据结构的第一个。因此，以下所有事务都将通过同一个 DHCP 服务器，直到某个事务在重试后失效。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。所有将要进行通信的控制器必须采用相同的 DHCP 代理设置。

注意：必须启用 DHCP 代理，以便 DHCP 选项 82 能够正常运行。

代理数据包流

代理数据包捕获

当控制器在DHCP代理模式时，不仅导向DHCP信息包对DHCP服务器，它实际上构件新的DHCP信息包转发到DHCP服务器。客户端 DHCP 数据包中的所有 DHCP 选项将复制到控制器的 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

此屏幕画面从客户端的方面采取的是数据包捕获。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bootp协议详细资料展开，显示DHCP选项。

服务器角度

此屏幕截图描述的是从服务器角度截取的数据包捕获过程。类似于前一示例，它显示了 DHCP 发现，DHCP 提供、DHCP 请求和 DHCP ACK。不过，这些都是控制器在充当 DHCP 代理时构建的数据包。再次，DHCP 请求突出显示，并且 bootp 协议详细资料展开，显示 DHCP 选项。请注意，它们与客户端 DHCP 请求数据包中的内容相同。并且请注意 WLC 代理中继信息包和优点数据包地址。

代理配置示例

为了使用控制器作为 DHCP 代理，在控制器必须启用 DHCP 代理功能。默认情况下会启用此功能。为了启用 DHCP 代理，可以使用此 CLI 命令。同样是可用的在控制器页的 GUI 在 DHCP 菜单。

```
(Cisco Controller) >config dhcp proxy enable (Cisco Controller) >show dhcp proxy DHCP Proxy Behavior: enabled
```

要运行 DHCP 代理，必须在需要 DHCP 服务的每个控制器接口上配置一个主 DHCP 服务器。可以在管理接口、AP 管理器接口和动态接口上配置 DHCP 服务器。这些 CLI 命令可以用于为了配置每个接口的一个 DHCP 服务器。

```
(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 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

以下是 `debug dhcp packet enable` 命令的输出。调试显示接收从一个客户端的 DHCP 请求有 MAC 地址的 00:40:96:b4:8c:e1，传达 DHCP 请求给 DHCP 服务器，收到从 DHCP 服务器的一回复，并且发送 DHCP 提供给客户端的控制器。

```
(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 = 50.101.2.7 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 - 11.0.0.11 (local address 50.101.0.11, gateway 50.101.0.1, 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: 50.101.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP requested ip: 50.101.2.7 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 50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REQUEST to 50.101.0.1 (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: 50.101.0.11 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 = 11.0.0.11 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 =
50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: DNS server, cnt = 1, first =
11.0.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: WINS server, cnt = 1, first =
11.0.0.11 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 11.0.0.11,
yiaddr 50.101.2.7) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 Assigning Address 50.101.2.7 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: 50.101.2.7 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: 1.1.1.1 rcvd server id: 11.0.0.11
```

警告

- 作为防火墙和DHCP服务器的互操作性问题能存在一个控制器之间用DHCP代理启用和设备。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。要解决此问题，需要在控制器上禁用 DHCP 代理。
- 当控制器上的客户端处于 DHCP REQ 状态时，控制器将丢弃 DHCP inform 数据包。在控制器从客户端收到 DHCP 发现数据包之前，控制器上的客户端不会进入 RUN 状态（要使客户端传送流量，这是必需的）。禁用 DHCP 代理时，将由控制器转发 DHCP inform 数据包。
- 所有将要进行通信的控制器必须采用相同的 DHCP 代理设置。

DHCP 桥接模式

DHCP 桥接功能旨在使控制器在 DHCP 事务中的作用对客户端完全透明。除对以太网II转换的 802.11外，从客户端的数据包桥接非限定从轻量级接入点协议(LWAPP)在IP (EoIP)通道的通道到客户端的VLAN (或以太网在漫游案件)的L3。同样，除了从以太网 II 到 802.11 的转换以外，传送到客户端的数据包将不加修改地从客户端的 VLAN (或 L3 漫游时的 EoIP 隧道) 桥接到 LWAPP 隧道。认为此作为配线客户端到switchport客户端然后执行传统DHCP处理。

[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画面，捕获在代理模式是DHCP服务器的实时IP的客户端之间的主要区别在提供和Ack数据包被看到而不是控制器的虚拟IP地址。

[桥接数据包捕获 - 服务器角度](#)

在有线的数据包捕获屏幕画面您能看到数据包40是从测试客户端广播的桥接的DHCP请求 00:40:96:b6:44:51对有线网络。

桥接配置示例

为了启用在控制器的DHCP桥接功能，您必须禁用在控制器的DHCP代理功能。这在CLI可能只完成用这些命令：

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

如果DHCP服务器在使用IP辅助，和一样客户端广播然后将需要转发到DHCP服务器在客户端网关的Layer2 (L2)网络不存在。以下是此配置的一个示例：

```
Switch#conf t Switch(config)#interface vlan <client vlan #> Switch(config-if)#ip helper-address <dhcp server IP>
```

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。您需要在有线基础架构中为控制器上的所有必需 VLAN 添加 IP 帮助程序语句。

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。

```
(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：

对DS的成功DHCP桥接信息包-这意味着从客户端的原始DHCP信息包桥接，未改变对分布式系统(DS)。DS 为有线基础架构。

对STA的成功DHCP桥接信息包-此消息表明DHCP信息包桥接，未改变到站点(STA)。STA是请求DHCP的客户端机器。

并且，您看到在调试列出的实际服务器IP地址，是192.168.10.1。如果桥接DHCP的代理是在使用中的而不是DHCP，您为服务器IP地址会看到列出的控制器的虚拟IP地址。

警告

- 默认情况下会启用 DHCP 代理。
- 所有将要进行通信的控制器必须采用相同的 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。它设计支持一个小无线网络用少于十接入点(AP)在相同子网。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，并且无法在较大规模的部署中进行扩展。

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。使用桥接控制器的 DHCP 操作更多类似有自治 AP 的 DHCP 上一步。DHCP 信息包通过与 VLAN 连接的客户端关联进入 AP 对服务集标识(SSID)。然后，DHCP 数据包会离开该 VLAN。如果 IP 辅助在该 VLAN 的第 3 层(L3)网关定义，数据包转发对该 DHCP 服务器通过处理的单播。DHCP 服务器然后响应上一步直接地对转发该 DHCP 信息包的 L3 接口。使用 DHCP 代理，它是同一个想法，但是所有转发完成直接地在控制器而不是 VLAN 的 L3 接口。例如，DHCP 请求从客户端进入 WLAN 后，WLAN 将使用在 VLAN 的接口上定义的 DHCP 服务器，或使用 WLAN 的 DHCP 覆盖功能，向 DHCP 服务器转发一个单播 DHCP 数据包，而 DHCP 数据包的 GIADDR 字段则使用 VLAN 接口的 IP 地址填充。

内部 DHCP 服务器 - 数据包流

内部 DHCP 服务器配置示例

您必须使控制器的 DHCP 代理为了允许内部 DHCP 服务器作用。可以通过以下 GUI 启用 DHCP 代理：

注意： 您不能通过在所有版本的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
```

为了启用内部DHCP服务器，请完成这些步骤：

1. 定义您将使用请求IP地址的范围(Controller>内部DHCP服务器> DHCP范围)。单击 **New**。
2. 指向任一您的DHCP覆盖您的控制器的管理接口IP地址。此外，您也可以将控制器接口配置的 DHCP 选项用于您希望使用内部 DHCP 服务器的接口。
3. 确保DHCP代理启用。

故障排除

内部DHCP服务器的调试典型地是找到有获得IP地址的一问题的客户端问题。您需要运行这些调试。

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

启用您的这些调试的调试客户端是宏，当仅集中调试于您输入了的客户端MAC地址时。

```
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
```

debug dhcp packet enable 命令是一个主要用于解决 DHCP 问题的命令，该命令由 **debug client** 命令自动启用。

```
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 = 1.1.1.1
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
```

清除在WLC's内部DHCP服务器的DHCP租约

您能发出此命令为了清除在WLC的内部DHCP服务器的DHCP租约：

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

示例如下：

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

警告

- 要运行内部 DHCP 服务器，必须启用 DHCP 代理。
- 使用对端口1067的DHCP，当您使用内部DHCP服务器，是受CPU ACL的影响的。
- 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

- `config dhcp proxy disable` 命令意指使用 DHCP 桥接功能。这是一个全局命令（不是基于 WLAN 的命令）。
- 为便于客户在使用现有部署时体验一致的行为，默认情况下将仍然启用 DHCP 代理。
- 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。实际桥接含义桥接，除802.11外对以太网II转换。DHCP信息包通过非限定从LWAPP通道到客户端的VLAN (和反过来也是一样地)。
- 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高级配置有要求用户在进入通过DHCP客户端能通过流量控制器)。的运转状态的一个选项(状态前此选项要求客户端执行整个或半个 DHCP 请求。控制器从客户端寻找的主要事件是DHCP请求和从DHCP服务器回来的ACK。只要客户端实行这些步骤，客户端通过DHCP所需的步骤并且移动向运转状态。

L2 和 L3 漫游

L2漫游-如果客户端有一有效DHCP租用并且执行L2漫游在同一L2网络的两个区别控制器之间，客户端不应该需要reDHCP，并且应该完全移动客户端条目向从原始控制器的新的控制器。然后，如果客户端需要再次进行 DHCP 操作，当前控制器上的 DHCP 桥接或代理进程将再次透明地桥接数据包。

L3漫游-在L3中请漫游客户端移动两个区别控制器之间用不同的L3网络的方案。在这种情况下，客户端将锚定到原始控制器并在新的外来控制器的客户端表中列出。在锚定期间，客户端的 DHCP 将由锚点控制器处理，因为客户端数据在外来控制器和锚点控制器之间的 EoIP 隧道内传输。

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](#)