Introduction

This document describes the different DHCP operations on the wireless controller, which provide consistent and accurate information to administrators who look to troubleshoot their network.

External DHCP Server

The Wireless LAN Controller (WLC) supports two modes of DHCP operations in case an external DHCP server is used:

- DHCP proxy mode
- DHCP bridging mode

DHCP proxy mode serves as a DHCP helper function in order to achieve better security and control over DHCP transactions between the DHCP server and the wireless clients. DHCP
bridging mode provides an option to make the controller’s role in a DHCP transaction entirely transparent to the wireless clients.

Comparison of DHCP Proxy and Bridging Modes

<table>
<thead>
<tr>
<th>Handling Client DHCP</th>
<th>DHCP Proxy Mode</th>
<th>DHCP Bridging Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify giaddr</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Modify siaddr</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Modify packet content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Redundant offers not forwarded</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Option 82 support</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Broadcast to unicast</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BOOTP support</td>
<td>No</td>
<td>Server</td>
</tr>
<tr>
<td>RFC non-compliant</td>
<td>Proxy and relay agent are not exactly the same concept. DHCP bridging mode is recommended for full RFC compliance.</td>
<td>No</td>
</tr>
</tbody>
</table>

DHCP Proxy Mode

The DHCP proxy is not ideal for all network environments. The controller modifies and relays all DHCP transactions to provide helper function and address certain security issues.

The controller’s virtual IP address is normally used as the source IP address of all DHCP transactions to the client. As a result, the real DHCP server IP address is not exposed in the air. This virtual IP is displayed in debug output for DHCP transactions on the controller. However, use of a virtual IP address can cause issues on certain types of clients.

DHCP proxy mode operation maintains the same behavior for both symmetric and asymmetric mobility protocols.

When multiple offers come from external DHCP servers, the DHCP proxy normally selects the first one that comes in and sets the IP address of the server in the client data structure. As a result, all following transactions go through the same DHCP server until a transaction fails after retries. At this point, the proxy selects a different DHCP server for the client.

DHCP proxy is enabled by default. All controllers that will communicate must have the same DHCP proxy setting.

**Note:** DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.

Proxy Packet flow

![DHCP Packet Flow Diagram](image-url)
Proxy Packet Capture

When the controller is in DHCP proxy mode, it not only directs DHCP packets to the DHCP server, it actually builds new DHCP packets to forward to the DHCP server. All DHCP options which are present in the client's DHCP packets are copied in the controller's DHCP packets. The next screenshot examples show this for a DHCP request packet.

Client Perspective

This screenshot is of a packet capture taken from the client's perspective. It shows a DHCP discover, DHCP offer, DHCP request, and a DHCP ACK. The DHCP request is highlighted and the bootp protocol detail is expanded, which shows the DHCP options.

Server Perspective

This screenshot is of a packet capture taken from the server's perspective. Similar to the previous example, it shows a DHCP discover, DHCP offer, DHCP request, and a DHCP ACK. However, these are packets that the controller built as a function of DHCP proxy. Again, the DHCP request is highlighted and the bootp protocol detail is expanded, which shows the DHCP options. Notice that they are the same as in the clients DHCP request packet. Also note that the WLC proxy relays packet and highlight packet addresses.
**Proxy Configuration Example**

In order to use the controller as a DHCP proxy, the DHCP proxy feature must be enabled on the controller. By default, this feature is enabled. In order to enable DHCP proxy, this CLI command can be used. The same is available in the GUI in the Controller page in the DHCP menu.

(Cisco Controller) >config dhcp proxy enable
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behavior: enabled

For DHCP proxy to work, a primary DHCP server must be configured on each controller interface that requires DHCP services. A DHCP server can be configured on the management interface, ap-manager interface, and on dynamic interfaces. These CLI commands can be used in order to configure a DHCP server for each interface.

(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>

The DHCP bridging feature is a global setting, so it affects all DHCP transactions within the controller.

**Troubleshoot**

This is the output of the `debug dhcp packet enable` command. The debug shows a controller that receives a DHCP request from a client with MAC address 00:40:96:b4:8c:e1, transmits a DHCP request to the DHCP server, receives a reply from the DHCP server, and sends a DHCP offer to the client.

(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 0x003)
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 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
(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)
secs: 0, flags: 0 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP dhcpaddr: 0.0.0.0, yiaddr: 0.0.0.0, yiaddr: 0.0.0.0 Thu Jun 25 21:48:55 2009:
Forwarding DHCP packet (332 octets)
--- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 50.101.0.1

- Interoperability issues can exist between a controller with DHCP proxy enabled and devices that act as both a firewall and DHCP server. This is most likely due to the firewall component of the device as firewalls generally do not respond to proxy requests. The workaround for this issue is to disable DHCP proxy on the controller.

- When a client is in DHCP REQ state on the controller, the controller drops DHCP inform packets. The client will not go into a RUN state on the controller (this is required for the client to pass traffic) until it receives a DHCP discover packet from the client. DHCP inform packets are forwarded by the controller when DHCP proxy is disabled.

- All controllers that will communicate must have the same DHCP proxy setting.

DHCP Bridging Mode

The DHCP bridging feature is designed to make the controller’s role in the DHCP transaction entirely transparent to the client. With the exception of 802.11 to Ethernet II conversion, packets from the client are bridged unmodified from the Light Weight Access Point Protocol ( Ethernet over IP (DHCP Bridging Operations - Bridging Packet Flow

![DHCP Bridging Operations - Bridging Packet Flow](image-url)
In the client side packet capture screenshot, the main difference between the client capture in Proxy mode is the real IP of the DHCP server is seen in the Offer and Ack packets instead of the controller’s virtual IP address.

Bridging Packet Capture - Server Perspective
In the wired packet capture screenshot you can see that packet 40 is the bridged DHCP Request broadcast from the test client 00:40:96:b6:44:51 to the wired network.

**Bridging Configuration Example**

In order to enable the DHCP bridging functionality on the controller, you must disable the DHCP proxy feature on the controller. This can only be accomplished in the CLI with these commands:

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

If the DHCP server does not exist on the same Layer 2 (L2) network as the client then the broadcast will need to be forwarded to the DHCP server at the client gateway using an IP helper. This is a sample of this configuration:

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

The DHCP bridging feature is a global setting, so it affects all DHCP transactions within the controller. You need to add IP helper statements in the wired infrastructure for all necessary VLANs on the controller.

**Troubleshoot**

The debugs listed here were enabled on the controller CLI and the DHCP portion of the output was extracted for this document.

(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 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)
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: 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: lease time = 86400 seconds
00:40:96:b6:44:51 DHCP option: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP options end, len 92, actual 84
00:40:96:b6:44:51 DHCP processing DHCP ACK (5)
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 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: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP options end, len 72, actual 64

In this DHCP debug output, there are a few key indications that DHCP bridging is in use on the controller:

DHCP successfully bridged packet to DS - This means that the original DHCP packet from the client was bridged, unaltered to the distribution system (DS). The DS is the wired infrastructure.

DHCP successfully bridged packet to STA - This message indicates that the DHCP packet was bridged, unaltered to the station (STA). The STA is the client machine that requests DHCP.

Also, you see the actual server IP address listed in the debugs, which is 192.168.10.1. If DHCP proxy was in use instead of DHCP bridging, you would see the controller’s virtual IP address listed for the server IP address.

Caveats
• By default, DHCP proxy is enabled.
• All controllers that will communicate must have the same DHCP proxy setting.
• DHCP proxy must be enabled for DHCP option 82 to work.

Internal DHCP Server

The internal DHCP server was introduced initially for branch offices where an external DHCP server is not available. It is designed to support a small wireless network with less than ten Access Points (APs) that are on the same subnet. The internal server provides IP addresses to wireless clients, direct-connect APs, appliance-mode APs on the management interface, and DHCP requests that are relayed from APs. It is not a full-blown general purpose DHCP server. It only supports limited functionality and will not scale in a larger deployment.

Comparison of Internal DHCP and Bridging Modes

The two main DHCP modes on the controller are either DHCP proxy or DHCP bridging. With DHCP bridging the controller acts more like a DHCP back with autonomous APs. A DHCP packet comes into the AP via a client association to a Service Set Identifier (SSID) that is linked to a VLAN. Then, the DHCP packet goes out that VLAN. If an IP helper is defined on that VLAN’s Layer 3 (L3) gateway, the packet is forwarded to that DHCP server via directed unicast. The DHCP server then responds back directly to the L3 interface that forwarded that DHCP packet. With DHCP proxy, it is the same idea, but all of the forwarding is done directly at the controller instead of the VLAN’s L3 interface. For example, a DHCP request comes in to the WLAN from the client, the WLAN then will either use the DHCP server defined on the VLAN’s interface “or” will use the DHCP override function of the WLAN to forward a unicast DHCP packet to the DHCP server with the DHCP packets GIADDR field filled out to be the VLAN interface’s IP address.

Internal DHCP Server - Packet flow

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.

Internal DHCP Server Configuration Example

You must enable DHCP proxy on the controller in order to allow the internal DHCP server to
function. This can be done via the GUI under this section:

**Note:** You are not able to set the DHCP proxy via the GUI in all versions.

(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
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
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
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)
DHCP Parameters

Enable DHCP Proxy
DHCP Option 82 Remote Id field format AP-MAC

Or via the CLI:

(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 option: chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP option: yiaddr: 0.0.0.0, yiaddr: 192.168.10.104
00:40:96:b6:44:51 DHCP option: siaddr: 0.0.0.0, giaddr: 0.0.0.0
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

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 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: 0x0224dfab6 (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 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: 0x0224dfab6 (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: 0x0224dfab6 (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 DHCP received op BOOTREPLY (1) (len 332, port 1, encap 0xec00)

In order to enable the internal DHCP server, complete these steps:

1. Define a scope that you will use to pull IP addresses (Controller > Internal DHCP Server > DHCP Scope). Click New.
2. Point either your DHCP override to the management interface IP address of your controller. Or, you can use the DHCP option of the controller interface configuration for the interface you wish to use the internal DHCP server.

3. Make sure that DHCP proxy is enabled.
Troubleshoot

A debug of the internal DHCP server is typically a matter of finding a client that has a problem getting an IP address. You need to run these debugs.

(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 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 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
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
DHCP option len (including the magic cookie) 72
DHCP option: message type = DHCP ACK
DHCP option: server id = 192.168.10.1
DHCP option: lease time = 86400 seconds
DHCP option: 58 (len 4) - skipping
DHCP option: 59 (len 4) - skipping
DHCP option: netmask = 255.255.255.0
DHCP option: gateway = 192.168.10.1
DHCP options end, len 72, actual 64
DHCP processing DHCP ACK (5)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
DHCP chaddr: 00:40:96:b6:44:51
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.10.104
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP server id: 192.168.10.1 rcvd server id: 192.168.10.1
Assigning Address 192.168.10.104 to mobile
DHCP successfully bridged packet to STA
DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03)
DHCP option len (including the magic cookie) 72
DHCP option: message type = DHCP DISCOVER
DHCP option: 116 (len 1) - skipping
DHCP option: 61 (len 7) - skipping
DHCP option: 12 (len 12) - skipping
DHCP option: vendor class id = MSFT 5.0 (len 8)
DHCP option: 55 (len 11) - skipping
DHCP options end, len 72, actual 64
DHCP processing DHCP DISCOVER (1)
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
DHCP chaddr: 00:40:96:b6:44:51
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP successfully bridged packet to DS
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
DHCP option len (including the magic cookie) 72
DHCP option: server id = 192.168.10.1
DHCP option: lease time = 86400 seconds
DHCP option: 58 (len 4) - skipping
DHCP option: 59 (len 4) - skipping
DHCP option: netmask = 255.255.255.0
DHCP option: gateway = 192.168.10.1
DHCP options end, len 72, actual 64
DHCP processing DHCP OFFER (2)
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
DHCP chaddr: 00:40:96:b6:44:51
DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.10.104
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
DHCP server id: 192.168.10.1 rcvd server id: 192.168.10.1
DHCP successfully bridged packet to STA
DHCP received op BOOTREQUEST (1) (len 328, port 1, encap 0xec03)
DHCP option len (including the magic cookie) 92
DHCP option: message type = DHCP REQUEST

The debug client is a macro that enables these debugs for you while it focuses the debug out only on the client MAC address that you have entered.

(debug client) >debug client 00:40:96:b6:44:51
(debug dhcp message enable)
DHCP option: 61 (len 7) - skipping
DHCP option: requested ip = 192.168.10.104
DHCP option: server id = 192.168.10.1
DHCP option: 12 (len 12) - skipping
DHCP option: 81 (len 16) - skipping
DHCP option: vendor class id = MSFT 5.0 (len 8)
DHCP option: 55 (len 11) - skipping
DHCP options end, len 92, actual 84
DHCP processing DHCP REQUEST (3)
DHCP option len (including the magic cookie) 72
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
DHCP option len (including the magic cookie) 81
DHCP option: message type = DHCP ACK
DHCP option: server id = 192.168.10.1
DHCP option: lease time = 86400 seconds
DHCP option: gateway = 192.168.100.1
DHCP option: 43 (len 3) - skipping
DHCP options end, len 81, actual 73
DHCP Forwarding packet locally (340 octets) from 192.168.100.254 to 192.168.100.104

The main one for DHCP issues is the `debug dhcp packet enable` command that is enabled automatically by the `debug client` command.
Clear the DHCP Leases on the WLC’s Internal DHCP Server

You can issue this command in order to clear the DHCP leases on the Internal DHCP server of the WLC:

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

Here is an example:

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

Caveats

- DHCP proxy must be enabled for the Internal DHCP server to function.
- Use of DHCP to port 1067 when you use the Internal DHCP server, which is affected by the CPU ACL.
- The Internal DHCP server listens on the controller loopback interface via 127.0.0.1 UDP port 67.

End User Interface

- The `config dhcp proxy disable` command implies the use of the DHCP bridging function. This is a global command (not a per-WLAN command).
- In order for customers to experience consistent behavior with existing deployments, the DHCP proxy will remain enabled by default.
- When the DHCP proxy is disabled, the Internal DHCP server cannot be used by local WLANs. The bridging operation is not consistent with the operations required to redirect a packet to the internal server. Bridging really does mean bridging, with the exception of 802.11 to Ethernet II conversion. DHCP packets are passed unmodified from the LWAPP tunnel to the client’s VLAN (and vice-versa).
- When the proxy is enabled, a DHCP server must be configured on the WLAN’s interface (or in the WLAN itself) in order for the WLAN to be enabled. No server needs to be configured when the proxy is disabled as these servers are not used.
- When a user attempts to enable the DHCP proxy, you internally verify that all WLANs (or associated interfaces) have a DHCP server configured. If not, the enable operation fails.
DHCP Required

The WLAN advanced configuration has an option that requires users to pass DHCP before going into the RUN state (a state where the client will be able to pass traffic through the controller). This option requires the client to do a full or half DHCP request. The main thing the controller looks for from the client is a DHCP request and an ACK that comes back from the DHCP server. As long as the client does these steps, the client passes the DHCP required step and moves to the RUN state.

L2 and L3 Roaming

L2 Roam - If the client has a valid DHCP lease and performs a L2 roam between two different controllers on the same L2 network, the client should not need to reDHCP and the client entry should be completely moved to the new controller from the original controller. Then, if the client does need to DHCP again, the DHCP bridging or proxy process on the current controller would transparently bridge the packet again.

L3 Roam - In a L3 roam scenario the client moves between two different controllers in different L3 networks. In this situation the client is anchored to the original controller and listed in the client table on the new foreign controller. During the anchoring scenario the client's DHCP is handled by the anchor controller as the client data is tunneled within an EoIP tunnel between the foreign and anchor controllers.

Related Information

- [DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example](#)
- [Technical Support & Documentation - Cisco Systems](#)