Configuring DHCP

- Restrictions for Configuring DHCP for WLANs, page 1
- Information About the Dynamic Host Configuration Protocol, page 1
- Configuring DHCP (GUI), page 3
- Configuring DHCP (CLI), page 4
- Debugging DHCP (CLI), page 4
- DHCP Client Handling, page 5

Restrictions for Configuring DHCP for WLANs

- The controller internal DHCP server does not support Cisco Aironet 600 Series OfficeExtend Access Point.
- Internal DHCP servers are not supported in Cisco Flex 7500 Series Controllers. As a workaround, you can use External DHCP servers.
- For WLANs with local switching and central DHCP feature enabled, clients with static IP addresses are not allowed. Enabling central DHCP will internally enable DHCP required option.

Information About the Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Internal DHCP Servers

The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains a maximum of 10 access points or fewer, with the access points on the same IP subnet as the controller. The internal server provides DHCP addresses to wireless clients, direct-connect access points, and DHCP requests that are relayed from access
points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the controller, such as local subnet broadcast, Domain Name System (DNS), or priming.

An internal DHCP server pool only serves the wireless clients of that controller, not clients of other controllers. Also, an internal DHCP server can serve only wireless clients, not wired clients.

When clients use the internal DHCP server of the controller, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign controller.

---

**Note**

DHCPv6 is not supported in the internal DHCP servers.

---

**External DHCP Servers**

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each controller appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the controller captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra controller, inter controller, and inter-subnet client roaming.

---

**Note**

External DHCP servers can support DHCPv6.

---

**DHCP Assignments**

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides the DHCP server address on the interface assigned to the WLAN.

**Security Considerations**

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.
Note

- WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.

- If your Cisco Aironet 1830 Series or Cisco Aironet 1850 Series AP does not receive an IP address through DHCP, the AP is assigned a default IP address from the 6.x.x.x range. Executing the show cdp neighbor command on a connected switch displays this IP address in the AP’s CDP neighbor table.

After DHCP issues, if any, are resolved, the AP is reassigned an IP address from the DHCP pool.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note

DHCP Addr. Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the controller. You must not define the primary/secondary configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Configuring DHCP (GUI)

To configure a primary DHCP server for a management, AP-manager, or dynamic interface, see the Configuring Ports and Interfaces chapter.

When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

Step 1
Choose WLANs to open the WLANs page.

Step 2
Click the ID number of the WLAN for which you want to assign an interface. The WLANs > Edit (General) page appears.

Step 3
On the General tab, unselect the Status check box and click Apply to disable the WLAN.

Step 4
Reclick the ID number of the WLAN.

Step 5
On the General tab, choose the interface for which you configured a primary DHCP server to be used with this WLAN from the Interface drop-down list.

Step 6
Choose the Advanced tab to open the WLANs > Edit (Advanced) page.

Step 7
If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, select the DHCP Server Override check box and enter the IP address of the desired DHCP server in the DHCP Server IP Addr text box. The default value for the check box is disabled.

Note
The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override.

Note
DHCP Server override is applicable only for the default group.
If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

**Note** If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

**Step 8**
If you want to require all clients to obtain their IP addresses from a DHCP server, select the **DHCP Addr. Assignment Required** check box. When this feature is enabled, any client with a static IP address is not allowed on the network. The default value is disabled.

**Note** DHCP Addr. Assignment Required is not supported for wired guest LANs.

**Note** PMIPv6 supports only DHCP based clients and Static IP address is not supported.

**Step 9**
Click **Apply**.

**Step 10**
On the General tab, select the **Status** check box and click **Apply** to reenable the WLAN.

**Step 11**
Click **Save Configuration**.

---

**Configuring DHCP (CLI)**

**Step 1**
Disable the WLAN by entering this command:

```
config wlan disable wlan-id
```

**Step 2**
Specify the interface for which you configured a primary DHCP server to be used with this WLAN by entering this command:

```
config wlan interface wlan-id interface_name
```

**Step 3**
If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, enter this command:

```
config wlan dhcp_server wlan-id dhcp_server_ip_address
```

**Note** The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the `show wlan` command to verify that the DHCP server has been assigned to the WLAN.

**Note** If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

**Note** PMIPv6 supports only DHCP based clients and Static IP address is not supported.

**Step 4**
Reenable the WLAN by entering this command:

```
config wlan enable wlan-id
```

---

**Debugging DHCP (CLI)**

Use these commands to debug DHCP:

```bash
show dhcp
show dhcp client
show error
show debug
```
• `debug dhcp packet {enable | disable}`—Enables or disables debugging of DHCP packets.

• `debug dhcp message {enable | disable}`—Enables or disables debugging of DHCP error messages.

• `debug dhcp service-port {enable | disable}`—Enables or disables debugging of DHCP packets on the service port.

**DHCP Client Handling**

Cisco WLC supports two modes of DHCP operations in case an external DHCP server is used, DHCP proxy mode and DHCP bridging mode.

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

**Table 1: 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>Per WLAN configurable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RFC Non-compliant</td>
<td>Proxy and relay agent are not exactly the same concept. But DHCP bridging mode is recommended for full RFC compliance.</td>
<td>No</td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. To enable client profiling, you must enable the DHCP required flag and disable the local authentication flag.

2. To configure a DHCP timeout value, use the config dhcp timeout command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>To enable client profiling, you must enable the <strong>DHCP required</strong> flag and disable the local authentication flag.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure a DHCP timeout value, use the <strong>config dhcp timeout</strong> command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the WLC will wait for a client to get a DHCP lease through DHCP.</td>
<td></td>
</tr>
</tbody>
</table>