



## DHCP for WLANs

---

- [Information About Dynamic Host Configuration Protocol, on page 1](#)
- [Restrictions for Configuring DHCP for WLANs, on page 4](#)
- [Guidelines for DHCP Relay Configuration, on page 4](#)
- [How to Configure DHCP for WLANs, on page 5](#)
- [Configuring the Internal DHCP Server, on page 7](#)
- [Configuring DHCP-Required for FlexConnect, on page 17](#)

## Information About 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 device contains an internal DHCP server. This server is typically used in branch offices that do not have a DHCP server.

A wireless network generally contains a maximum of 10 APs or less, with the APs on the same IP subnet as the device.

The internal server provides DHCP addresses to wireless clients, direct-connect APs, and DHCP requests that are relayed from APs. Only lightweight APs are supported. If you want to use the internal DHCP server, ensure that you configure SVI for the client VLAN, and set the IP address as DHCP server IP address.

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

When clients use the internal DHCP server of the device, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned to 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 device.



- 
- Note**
- VRF is not supported in the internal DHCP servers.
  - DHCPv6 is not supported in the internal DHCP servers.
- 

### General Guidelines

- Internal DHCP server serves both wireless client and wired client (wired client includes AP).
- To serve wireless client with internal DHCP server, an unicast DHCP server IP address must be configured for wireless client. Internal DHCP server IP address must be configured under the server facing interface, which can be loopback interface, SVI interface, or L3 physical interface.
- To use internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under client VLAN SVI interface.
- For wireless client, in DHCP helper address configuration, the IP address of the internal DHCP server must be different from address of wireless client VLAN SVI interface.
- For wireless client with internal DHCP server support, the internal DHCP server can be configured using global configuration command, under the client VLAN SVI interface or under the wireless policy profile.
- An internal DHCP server pool can also serve clients of other controllers .

## 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 in 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 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 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 ask all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all the WLANs with a DHCP Address Assignment Required setting, which disallows client static IP addresses. If DHCP Address Assignment Required is selected, clients must obtain an IP address through 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.
  - 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. This means that each controller appears as a DHCP relay to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

---

You can create WLANs with DHCP Address Assignment Required disabled. If you do this, clients have the option of using a static IP address or obtaining an IP address from a designated DHCP server. However, note that this might compromise security.



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

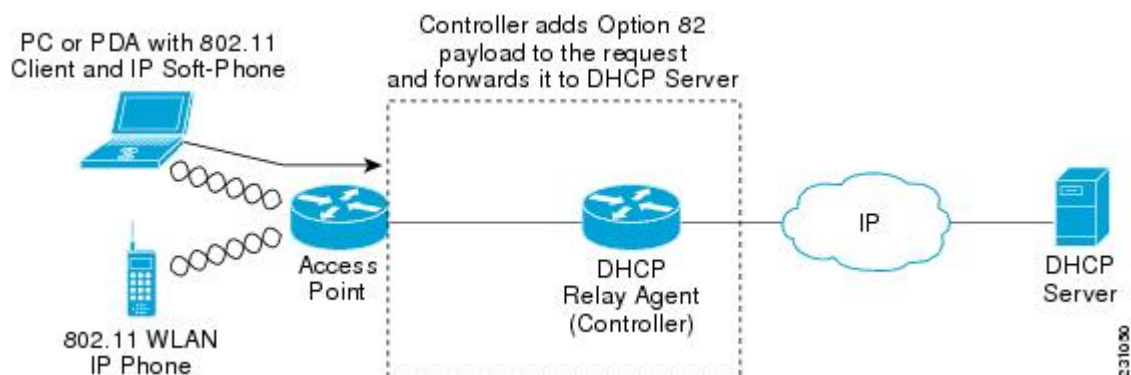
---

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

## DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the controller to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 1: DHCP Option 82



The AP forwards all the DHCP requests from a client to the controller. The controller adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the AP, depending on how you configure this option.



**Note** DHCP packets that already include a relay agent option are dropped at the controller.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.

## Restrictions for Configuring DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the controller.

You can configure DHCP service in either of the following ways:

- Configuring the DHCP pool on the controller.
- Configuring a DHCP relay agent on the SVI. Note that the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

## Guidelines for DHCP Relay Configuration

### Relay Agent Source IP

- If you configure source interface VLAN in the SVI interface, the IP address of the VLAN interface configured as source is used.
- If the Relay Agent source IP is not mentioned, the IP address of the SVI interface created for the corresponding client's VLAN is used.
- If the Relay Agent source IP is not mentioned, the source address specified at the global level is used.

**Note**

- The DHCP packets are sourced from the IP address of the Wireless Management Interface (WMI), if VLAN is not configured in the policy profile and AAA override.
- The SVI interface configuration is mandatory to achieve the DHCP relay functionality in central DHCP or local switching.
- Even though many interface options are available in the **ip dhcp relay source-interface** <> command, only VLAN interface is applicable.

**DHCP Server**

- If the DHCP server address is configured in the wireless policy profile, the server address configured in the policy profile takes precedence.
- If the DHCP server address is not configured in the policy profile, the server address configured in SVI takes precedence.

**Note**

You can configure two server addresses in the SVI. In this case, the DHCP packets from the client are sent to both the servers.

The Option 82 configured in policy profile, SVI, and globally is considered and honored together.

# How to Configure DHCP for WLANs

## Configuring DHCP Scopes (GUI)

**Procedure**

- Step 1** Choose **Administration > DHCP Pools**.
- Step 2** In the **Pools** section, click **Add** to add a new DHCP pool.  
The **Create DHCP Pool** dialog box is displayed.
- Step 3** In the **DHCP Pool Name** field, enter a name for the new DHCP pool.
- Step 4** From the **IP Type** drop-down list, choose the IP address type.
- Step 5** In the **Network** field, enter the network served by this DHCP scope. This IP address is used by the management interface with netmask applied, as configured in the **Interfaces** window.
- Step 6** In the **Subnet Mask** field, enter the subnet mask assigned to all the wireless clients.
- Step 7** In the **Starting ip** field, enter the starting IP address.
- Step 8** In the **Ending ip** field, enter the trailing IP address.
- Step 9** In the **Reserved Only** field, enable or disable it.

- Step 10** From the **Lease** drop-down list, choose the lease type as either **User Defined** or **Never Expires**. If you choose User Defined, you can enter the amount of time that an IP address is granted to a client.
- Step 11** To perform advanced configuration for DHCP scope, click **Advanced**.
- Step 12** Check the **Enable DNS Proxy** check box to enable DNS proxy.
- Step 13** In the **Default Router(s)** field, enter the IP address of the optional router or routers that connect to the device and click the + icon to add them to the list. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.
- Step 14** In the **DNS Server(s)** field, enter the IP address of the optional DNS server or servers and click the + icon to add them to the list. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by the DHCP scope.
- Step 15** In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name server or servers, such as Microsoft Windows Internet Naming Service (WINS) server, and click the + icon to add them to the list.
- Step 16** In the **Domain** field, enter the optional domain name of the DHCP scope for use with one or more DNS servers.
- Step 17** To add **DHCP** options, click **Add** in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information, such as DHCP options, to the clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.
- Step 18** Enter the **DHCP** option that you want to add.
- Step 19** Click **Save & Apply to Device**.

## Configuring DHCP Scopes (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ip dhcp pool <i>pool-name</i></b> <b>Example:</b> Device(config)# ip dhcp pool test-pool	Configures the DHCP pool address.
<b>Step 3</b>	<b>network <i>network-name mask-address</i></b> <b>Example:</b> Device(dhcp-config)# network 209.165.200.224 255.255.255.0	Specifies the network number in dotted-decimal notation and the mask address.
<b>Step 4</b>	<b>dns-server <i>hostname</i></b> <b>Example:</b> Device(dhcp-config)# dns-server example.com	Specifies the DNS name server. You can specify an IP address or a hostname.

	Command or Action	Purpose
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device (dhcp-config) # end	Returns to privileged EXEC mode.

## Configuring the Internal DHCP Server

### Configuring the Internal DHCP Server Under Client VLAN SVI (GUI)

#### Procedure

- 
- Step 1** Choose **Configuration > Layer2 > VLAN > SVI**.
  - Step 2** Click an SVI.
  - Step 3** Click the **Advanced** tab.
  - Step 4** Under **DHCP Relay** settings, enter the **IPV4 Helper Address**.
  - Step 5** Click **Update & Apply to Device**.
- 

### Configuring the Internal DHCP Server Under Client VLAN SVI (CLI)

#### Before you begin

- For wireless clients, only two DHCP servers are supported.
- To use the internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under the client VLAN SVI.
- For wireless clients, the IP address of the internal DHCP server must be different from the address of the wireless client VLAN SVI (in the DHCP helper address configuration).
- For wireless clients, the internal DHCP server can be configured under the client VLAN SVI or under the wireless policy profile.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface loopback interface-number</b>  <b>Example:</b>	Creates a loopback interface and enters interface configuration mode.

	Command or Action	Purpose
	Device (config)# interface Loopback0	
<b>Step 3</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device (config-if)# ip address 10.10.10.1 255.255.255.255	Configures the IP address for the interface.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device (config-if)# exit	Exits interface configuration mode.
<b>Step 5</b>	<b>interface vlan</b> <i>vlan-id</i> <b>Example:</b> Device (config)# interface vlan 32	Configures the VLAN ID.
<b>Step 6</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device (config-if)# ip address 192.168.32.100 255.255.255.0	Configures the IP address for the interface.
<b>Step 7</b>	<b>ip helper-address</b> <i>ip-address</i> <b>Example:</b> Device (config-if)# ip helper-address 10.10.10.1	Configures the destination address for UDP broadcasts. <b>Note</b> If the IP address used in the <b>ip helper-address</b> command is an internal address of the controller an internal DHCP server is used. Otherwise, the external DHCP server is used.
<b>Step 8</b>	<b>no mop enabled</b> <b>Example:</b> Device (config-if)# no mop enabled	Disables the Maintenance Operation Protocol (MOP) for an interface.
<b>Step 9</b>	<b>no mop sysid</b> <b>Example:</b> Device (config-if)# no mop sysid	Disables the task of sending MOP periodic system ID messages.
<b>Step 10</b>	<b>exit</b> <b>Example:</b> Device (config-if)# exit	Exits interface configuration mode.
<b>Step 11</b>	<b>ip dhcp excluded-address</b> <i>ip-address</i> <b>Example:</b> Device (config)# ip dhcp excluded-address 192.168.32.1	Specifies the IP address that the DHCP server should not assign to DHCP clients.



	Command or Action	Purpose
<b>Step 12</b>	<b>ip dhcp excluded-address</b> <i>ip-address</i> <b>Example:</b> Device(config)# ip dhcp excluded-address 192.168.32.100	Specifies the IP addresses that the DHCP server should not assign to DHCP clients.
<b>Step 13</b>	<b>ip dhcp pool</b> <i>pool-name</i> <b>Example:</b> Device(config)# ip dhcp pool pool-vlan32	Configures the DHCP pool address.
<b>Step 14</b>	<b>network</b> <i>network-name mask-address</i> <b>Example:</b> Device(dhcp-config)# network 192.168.32.0 255.255.255.0	Specifies the network number in dotted-decimal notation, along with the mask address.
<b>Step 15</b>	<b>default-router</b> <i>ip-address</i> <b>Example:</b> Device(dhcp-config)# default-router 192.168.32.1	Specifies the IP address of the default router for a DHCP client.
<b>Step 16</b>	<b>exit</b> <b>Example:</b> Device(dhcp-config)# exit	Exits DHCP configuration mode.
<b>Step 17</b>	<b>wireless profile policy</b> <i>profile-policy</i> <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Configures the WLAN policy profile and enters wireless policy configuration mode.
<b>Step 18</b>	<b>central association</b> <b>Example:</b> Device(config-wireless-policy)# central association	Configures central association for locally switched clients.
<b>Step 19</b>	<b>central dhcp</b> <b>Example:</b> Device(config-wireless-policy)# central dhcp	Configures the central DHCP for locally switched clients.
<b>Step 20</b>	<b>central switching</b> <b>Example:</b> Device(config-wireless-policy)# central switching	Configures WLAN for central switching.
<b>Step 21</b>	<b>description</b> <i>policy-profile-name</i> <b>Example:</b> Device(config-wireless-policy)# description "default policy profile"	Adds a description for the policy profile

	Command or Action	Purpose
<b>Step 22</b>	<b>vlan</b> <i>vlan-name</i>  <b>Example:</b> Device(config-wireless-policy)# vlan 32	Assigns the profile policy to the VLAN.
<b>Step 23</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the wireless profile policy.

## Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
  - Step 2** Click a policy name.
  - Step 3** Click the **Advanced** tab.
  - Step 4** Under **DHCP** settings, check or uncheck the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.
  - Step 5** Click **Update & Apply to Device**.
- 

## Configuring the Internal DHCP Server Under a Wireless Policy Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface loopback</b> <i>interface-number</i>  <b>Example:</b> Device(config)# interface Loopback0	Creates a loopback interface and enters interface configuration mode.
<b>Step 3</b>	<b>ip address</b> <i>ip-address</i>  <b>Example:</b> Device(config-if)# ip address 10.10.10.1 255.255.255.255	Configures the IP address for the interface.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b>	Exits interface configuration mode.

	Command or Action	Purpose
	Device(config-if)# exit	
<b>Step 5</b>	<b>interface vlan</b> <i>vlan-id</i> <b>Example:</b> Device(config)# interface vlan 32	Configures the VLAN ID.
<b>Step 6</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device(config-if)# ip address 192.168.32.100 255.255.255.0	Configures the IP address for the interface.
<b>Step 7</b>	<b>no mop enabled</b> <b>Example:</b> Device(config-if)# no mop enabled	Disables the Maintenance Operation Protocol (MOP) for an interface.
<b>Step 8</b>	<b>no mop sysid</b> <b>Example:</b> Device(config-if)# no mop sysid	Disables the task of sending MOP periodic system ID messages.
<b>Step 9</b>	<b>exit</b> <b>Example:</b> Device(config-if)# exit	Exits interface configuration mode.
<b>Step 10</b>	<b>ip dhcp excluded-address</b> <i>ip-address</i> <b>Example:</b> Device(config)# ip dhcp excluded-address 192.168.32.100	Specifies the IP address that the DHCP server should not assign to DHCP clients.
<b>Step 11</b>	<b>ip dhcp pool</b> <i>pool-name</i> <b>Example:</b> Device(config)# ip dhcp pool pool-vlan32	Configures the DHCP pool address.
<b>Step 12</b>	<b>network</b> <i>network-name mask-address</i> <b>Example:</b> Device(dhcp-config)# network 192.168.32.0 255.255.255.0	Specifies the network number in dotted-decimal notation along with the mask address.
<b>Step 13</b>	<b>default-router</b> <i>ip-address</i> <b>Example:</b> Device(dhcp-config)# default-router 192.168.32.1	Specifies the IP address of the default router for a DHCP client.
<b>Step 14</b>	<b>exit</b> <b>Example:</b> Device(dhcp-config)# exit	Exits DHCP configuration mode.

	Command or Action	Purpose
<b>Step 15</b>	<b>wireless profile policy</b> <i>profile-policy</i> <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Configures a WLAN policy profile and enters wireless policy configuration mode.
<b>Step 16</b>	<b>central association</b> <b>Example:</b> Device(config-wireless-policy)# central association	Configures central association for locally switched clients.
<b>Step 17</b>	<b>central switching</b> <b>Example:</b> Device(config-wireless-policy)# central switching	Configures local switching.
<b>Step 18</b>	<b>description</b> <i>policy-profile-name</i> <b>Example:</b> Device(config-wireless-policy)# description "default policy profile"	Adds a description for the policy profile.
<b>Step 19</b>	<b>ipv4 dhcp opt82</b> <b>Example:</b> Device(config-wireless-policy)# ipv4 dhcp opt82	Enables DHCP Option 82 for the wireless clients.
<b>Step 20</b>	<b>ipv4 dhcp opt82 ascii</b> <b>Example:</b> Device(config-wireless-policy)# ipv4 dhcp opt82 ascii	Enables ASCII on DHCP Option 82.
<b>Step 21</b>	<b>ipv4 dhcp opt82 format vlan_id</b> <b>Example:</b> Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32	Enables VLAN ID.
<b>Step 22</b>	<b>ipv4 dhcp opt82 rid</b> <i>vlan_id</i> <b>Example:</b> Device(config-wireless-policy)# ipv4 dhcp opt82 rid	Supports the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82.
<b>Step 23</b>	<b>ipv4 dhcp server</b> <i>ip-address</i> <b>Example:</b> Device(config-wireless-policy)# ipv4 dhcp server 10.10.10.1	Configures the WLAN's IPv4 DHCP server.
<b>Step 24</b>	<b>vlan</b> <i>vlan-name</i> <b>Example:</b>	Assigns the profile policy to the VLAN.

	Command or Action	Purpose
	Device(config-wireless-policy)# vlan 32	
<b>Step 25</b>	<b>no shutdown</b>  <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the wireless profile policy.

## Configuring the Internal DHCP Server Globally (GUI)

### Procedure

- 
- Step 1** Choose **Administration > DHCP Pools > Pools**.
- Step 2** Click **Add**.  
The **Create DHCP Pool** window is displayed.
- Step 3** Enter the **DHCP Pool Name**, **Network**, **Starting ip**, and **Ending ip**.
- Step 4** From the **IP Type**, **Subnet Mask**, and **Lease** drop-down lists, choose a value.
- Step 5** Click the **Reserved Only** toggle button.
- Step 6** Click **Apply to Device**.
- 

## Configuring the Internal DHCP Server Globally (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>interface loopback <i>interface-num</i></b>  <b>Example:</b> Device(config)# interface Loopback0	Creates a loopback interface and enters interface configuration mode.
<b>Step 3</b>	<b>ip address <i>ip-address</i></b>  <b>Example:</b> Device(config-if)# ip address 10.10.10.1 255.255.255.255	Configures the IP address for the interface.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits interface configuration mode.

	Command or Action	Purpose
<b>Step 5</b>	<b>interface</b> <i>vlan</i> <i>vlan-id</i> <b>Example:</b> Device(config)# interface vlan 32	Configures the VLAN ID.
<b>Step 6</b>	<b>ip address</b> <i>ip-address</i> <b>Example:</b> Device(config-if)# ip address 192.168.32.100 255.255.255.0	Configures the IP address for the interface.
<b>Step 7</b>	<b>no mop enabled</b> <b>Example:</b> Device(config-if)# no mop enabled	Disables the Maintenance Operation Protocol (MOP) for an interface.
<b>Step 8</b>	<b>no mop sysid</b> <b>Example:</b> Device(config-if)# no mop sysid	Disables the task of sending the MOP periodic system ID messages.
<b>Step 9</b>	<b>exit</b> <b>Example:</b> Device(config-if)# exit	Exits the interface configuration mode.
<b>Step 10</b>	<b>ip dhcp-server</b> <i>ip-address</i> <b>Example:</b> Device(config)# ip dhcp-server 10.10.10.1	Specifies the target DHCP server parameters.
<b>Step 11</b>	<b>ip dhcp excluded-address</b> <i>ip-address</i> <b>Example:</b> Device(config)# ip dhcp excluded-address 192.168.32.100	Specifies the IP address that the DHCP server should not assign to DHCP clients.
<b>Step 12</b>	<b>ip dhcp pool</b> <i>pool-name</i> <b>Example:</b> Device(config)# ip dhcp pool pool-vlan32	Configures the DHCP pool address.
<b>Step 13</b>	<b>network</b> <i>network-name mask-address</i> <b>Example:</b> Device(dhcp-config)# network 192.168.32.0 255.255.255.0	Specifies the network number in dotted-decimal notation along with the mask address.
<b>Step 14</b>	<b>default-router</b> <i>ip-address</i> <b>Example:</b> Device(dhcp-config)# default-router 192.168.32.1	Specifies the IP address of the default router for a DHCP client.

	Command or Action	Purpose
<b>Step 15</b>	<b>exit</b> <b>Example:</b> Device(dhcp-config)# exit	Exits DHCP configuration mode.
<b>Step 16</b>	<b>wireless profile policy <i>profile-policy</i></b> <b>Example:</b> Device(config)# wireless profile policy default-policy-profile	Configures a WLAN policy profile and enters wireless policy configuration mode.
<b>Step 17</b>	<b>central association</b> <b>Example:</b> Device(config-wireless-policy)# central association	Configures central association for locally switched clients.
<b>Step 18</b>	<b>central dhcp</b> <b>Example:</b> Device(config-wireless-policy)# central dhcp	Configures central DHCP for locally switched clients.
<b>Step 19</b>	<b>central switching</b> <b>Example:</b> Device(config-wireless-policy)# central switching	Configures local switching.
<b>Step 20</b>	<b>description <i>policy-profile-name</i></b> <b>Example:</b> Device(config-wireless-policy)# description "default policy profile"	Adds a description for the policy profile.
<b>Step 21</b>	<b>vlan <i>vlan-name</i></b> <b>Example:</b> Device(config-wireless-policy)# vlan 32	Assigns the profile policy to the VLAN.
<b>Step 22</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)# no shutdown	Enables the profile policy.

## Verifying Internal DHCP Configuration

To verify client binding, use the following command:

```
Device# show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type      State
Interface
                Hardware address/
```

```

User name
192.168.32.3    0130.b49e.491a.53    Mar 23 2018 06:42 PM    Automatic    Active
Loopback0

```

To verify the DHCP relay statistics for a wireless client, use the following command:

```
Device# show wireless dhcp relay statistics
```

```

DHCP Relay Statistics
-----

DHCP Server IP :    10.10.10.1

Message                Count
-----
DHCPDISCOVER           :    1
BOOTP FORWARD          :   137
BOOTP REPLY             :    0
DHCPOFFER              :    0
DHCPREQUEST            :   54
DHCPACK                :    0
DHCPNAK                :    0
DHCPDECLINE            :    0
DHCPRELEASE            :    0
DHCPINFORM             :   82

Tx/Rx Time :
-----
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-----
TxDropCount : 0

```

To verify the DHCP packet punt statistics in CPP, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless punt statistics
```

```

CPP Wireless Punt stats:

App Tag                Packet Count
-----
CAPWAP_PKT_TYPE_DOT11_PROBE_REQ    14442
CAPWAP_PKT_TYPE_DOT11_MGMT          50
CAPWAP_PKT_TYPE_DOT11_IAPP         9447
CAPWAP_PKT_TYPE_DOT11_RFID          0
CAPWAP_PKT_TYPE_DOT11_RRM           0
CAPWAP_PKT_TYPE_DOT11_DOT1X         0
CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE    2191
CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE  0
CAPWAP_PKT_TYPE_CAPWAP_CNTRL        7034
CAPWAP_PKT_TYPE_CAPWAP_DATA          0
CAPWAP_PKT_TYPE_MOBILITY_CNTRL      0
WLS_SMD_WEBAUTH                    0
SISF_PKT_TYPE_ARP                   5292
SISF_PKT_TYPE_DHCP                   140
SISF_PKT_TYPE_DHCP6                 1213
SISF_PKT_TYPE_IPV6_ND                 350
SISF_PKT_TYPE_DATA_GLEAN              44
SISF_PKT_TYPE_DATA_GLEAN_V6          51
SISF_PKT_TYPE_DHCP_RELAY             122

```



CAPWAP\_PKT\_TYPE\_CAPWAP\_RESERVED

0

# Configuring DHCP-Required for FlexConnect

## Information About FlexConnect DHCP-Required

The DHCP-Required knob on a policy profile forces a connected wireless client to get the IP address from DHCP. When the client completes the DHCP process and acquires an IP address, this IP address is learnt by the controller and only then the client traffic is switched on to the network. The DHCP-Required feature is already supported in central switching.

In Cisco IOS XE Amsterdam 17.2.1, the feature is supported on FlexConnect local switching clients. Prior to Release 17.2.1, DHCP-Required was not enforced on FlexConnect local switching clients. The IP address learnt by the AP or the controller for the wireless client is tracked to create an IP-MAC binding. As part of this feature, when a FlexConnect local switching client roams from one AP to another, the client need not do the DHCP again in the same L2 network, because the controller tracks the IP address and pushes the binding to the newly roaming AP.

The FlexConnect DHCP-Required feature can be configured from open configuration models, CLI, and from the GUI. The CLI and GUI configurations are described in this chapter. For more information about the open configuration modes, see the [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/172/b\\_172\\_programmability\\_cg.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/172/b_172_programmability_cg.html).

## Restrictions and Limitations for FlexConnect DHCP-Required

The following are the restrictions and limitations for the FlexConnect DHCP-Required feature:

- The DHCP-Required feature is applicable for IPv4 addresses only.
- The IP-MAC binding can be pushed to other APs only through the custom policy profile. IP-MAC binding is not available in the default policy. The mapping is propagated to all the APs in the same custom policy profile.
- The DHCP-Required feature works on IP-MAC binding basis and is not supported with third party workgroup bridge (WGB), where WGB wired client information is not shared to AP by the WGB.
- Cisco Wave 2 APs take 180 seconds to remove a client entry with static IP, when DHCP-required is enabled.

## Configuring FlexConnect DHCP-Required (GUI)

Perform the steps given below to configure the FlexConnect DHCP-Required feature through the GUI:

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Policy**.
- Step 2** On the **Policy** window, click the name of the corresponding Policy Profile. The **Edit Policy Profile** window is displayed.

- Step 3** Click the **Advanced** tab.
- Step 4** In the **DHCP** section, check the **IPv4 DHCP Required** check box to enable the feature.
- Step 5** Click **Update & Apply to Device**.

## Configuring FlexConnect DHCP-Required (CLI)

Perform the procedure given below to configure FlexConnect DHCP-Required through the CLI:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device#configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile policy profile-policy</b> <b>Example:</b> Device#wireless profile policy rr-xyz-policy-1	Configures WLAN policy profile and enters the wireless policy configuration mode.
<b>Step 3</b>	<b>ipv4 dhcp required</b> <b>Example:</b> Device(config-wireless-policy)#ipv4 dhcp required	Enables the FlexConnect DHCP-Required feature.
<b>Step 4</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wireless-policy)#no shutdown	Saves the configuration.

## Verifying FlexConnect DHCP-Required

- To verify the IP address learnt for a client on an IP DHCP-Required policy-enabled WLAN, use the **show wireless client summary** command:



**Note** The controller or AP does not learn the IP address through other means such as ARP or data gleaning, when IPv4 DHCP-Required is enabled.

```
Device# show wireless client summary
Number of Clients: 1
MAC Address          AP Name              Type  ID  State          Protocol  Method
Role
-----
1cXX.bXXX.59XX      APXXXX.7XXX.4XXX    WLAN  3   IP Learn      11ac      Dot1x
Local
```

- This example shows that the client IP is in the **Run** state, indicating that the client has received the IP address from DHCP:

```
Device# show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol
Method	Role				
5XXX.37XX.c3XX	APXXXX.4XXX.4XXX	WLAN	3	Run	11n (5)
None	Local				

