

DHCP

- Information About Dynamic Host Configuration Protocol, on page 1
- DHCP Proxy Mode, on page 3
- DHCP Option 82, on page 7
- DHCP Option 82 Link Select and VPN Select Suboptions, on page 9
- Internal DHCP Server, on page 13

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 controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server.

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

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 to the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Note

- VRF is not supported in the internal DHCP servers.
- 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.
- 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 agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

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.

DHCP Proxy Mode versus DHCP Bridging Mode

When using external DHCP servers, the controller can operate in one of two modes: as a DHCP Relay or as a DHCP Bridge.

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

Handling Client DHCP	DHCP Proxy Mode	DHCP Bridging Mode
Modify giaddr	Yes	No
Modify siaddr	Yes	No
Modify Packet Content	Yes	No
Redundant offers not forwarded	Yes	No
Option 82 Support	Yes	No
Broadcast to Unicast	Yes	No
BOOTP support	No	Server
Per WLAN configurable	Yes	No
RFC Non-compliant	Proxy and relay agent are not exactly the same concept. But DHCP bridging mode is recommended for full RFC compliance.	No

DHCP Proxy Mode

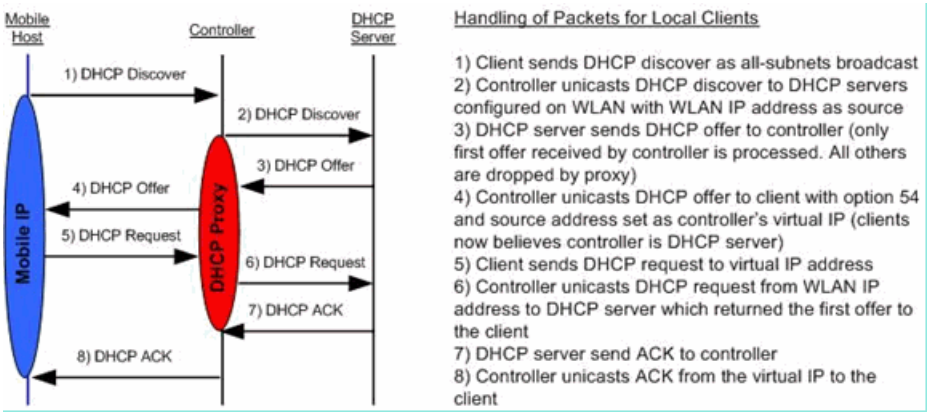
In DHCP Proxy Mode, the controller’s virtual IP address is used as the source IP address of all DHCP transactions to the client. As a result, the real DHCP server IP address is not exposed in the air. This virtual IP is displayed in debug output for DHCP transactions on the controller. However, use of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

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 in a mobility list must have the same DHCP proxy setting.

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

Proxy Mode Packet Flow



This section contains the following subsections:

Restrictions on Using DHCP Proxy

- DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.
- All controllers that will communicate must have the same DHCP proxy setting.
- DHCP v6 Proxy is not supported.
- Suppose an interface in an interface group is marked as *dirty*. If a client is mapped to this interface through its association with a WLAN mapped to the interface group, the client does not get mapped to a new interface in the interface group because the controller DHCP proxy does not update the client interface VLAN to a new interface. This has been observed in conditions in which the interface group is assigned through AAA override and the DHCP mode is aggressive. The workaround is to use a non-aggressive DHCP mode.

  For more information, see CSCvv74634.

Configuring DHCP Proxy (GUI)

Procedure

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **Enable DHCP Proxy** check box to enable DHCP proxy on a global basis. Otherwise, unselect the check box. The default value is selected.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring DHCP Proxy (GUI)

Procedure

Step 1 Choose **Controller > Interfaces**.

Step 2 Select the interface you want to configure the DHCP proxy.

You can configure the DHCP proxy on the management, virtual, ap manager, or dynamic interfaces in the controller.

The **Interfaces > Edit** page is displayed with DHCP information on the primary and secondary DHCP servers configured in the controller. If the primary and secondary servers are not listed, you must enter values for the IP address of the DHCP servers in the text boxes displayed in this window.

Step 3 Select from the following option of the proxy mode drop-down to enable DHCP proxy on the selected management interface:Global—Uses the global DHCP proxy mode on the controller.Enabled—Enables the DHCP proxy mode on the interface. When you enable DHCP proxy on the controller; the controller unicasts the DHCP requests from the client to the configured servers. You must configure at least one DHCP server on either the interface associated with the WLAN or on the WLAN.Disabled—Disables the DHCP proxy mode on the interface. When you disable the DHCP proxy on the controller, the DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled.

Step 4 Check the Enable DHCP option 82 checkbox to ensure additional security when DHCP is used to allocate network addresses, check the Enable DHCP option 82 checkbox.

Step 5 Click **Apply** to save the configuration.

Configuring DHCP Proxy (CLI)

Procedure

Step 1 Enable or disable DHCP proxy by entering this command:

config dhcp proxy {**enable** | **disable**}

Step 2 View the DHCP proxy configuration by entering this command:

show dhcp proxy

Information similar to the following appears:

```
DHCP Proxy Behavior: enabled
```

Configuring DHCP Proxy (CLI)

Procedure

Step 1 Configure the DHCP primary and secondary servers on the interface. To do this, enter the following commands:

- **config interface dhcp management primary** *primary-server*
- **config interface dhcp dynamic-interface** *interface-name* **primary primary-s**

Step 2 Configure DHCP proxy on the management or dynamic interface of the controller. To do this, enter the following command:

- **config interface dhcp management proxy-mode** enableglobaldisable
- **config interface dhcp dynamic-interface** *interface-name* **proxy-mode** enableglobaldisable.

Note
To ensure additional security when DHCP is configured, use the **config interface dhcp***interface type***option-82 enable** command.

Step 3 Enter the **save config** command.

Step 4 To view the proxy settings of the controller interface enter the **show dhcp proxy** command.

Configuring a DHCP Timeout (GUI)

For client associations to a WLAN that has DHCP required, the DHCP timeout controls how long the controller will wait, after a new association, for the client to complete DHCP. If the DHCP exchange is not completed within the timeout period, the controller deauthenticates the client. The default setting is the maximum of 120 seconds; we recommend that you do not reduce this value.

Procedure

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **DHCP Timeout (5 - 120 seconds)** check box to enable a DHCP timeout on a global basis. Otherwise, unselect the check box. The valid range is 5 through 120 seconds.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring a DHCP Timeout (CLI)

For client associations to a WLAN that has DHCP required, the DHCP timeout controls how long the controller will wait, after a new association, for the client to complete DHCP. If the DHCP exchange is not completed within the timeout period, the controller deauthenticates the client. The default setting is the maximum of 120 seconds; we recommend that you do not reduce this value.

Procedure

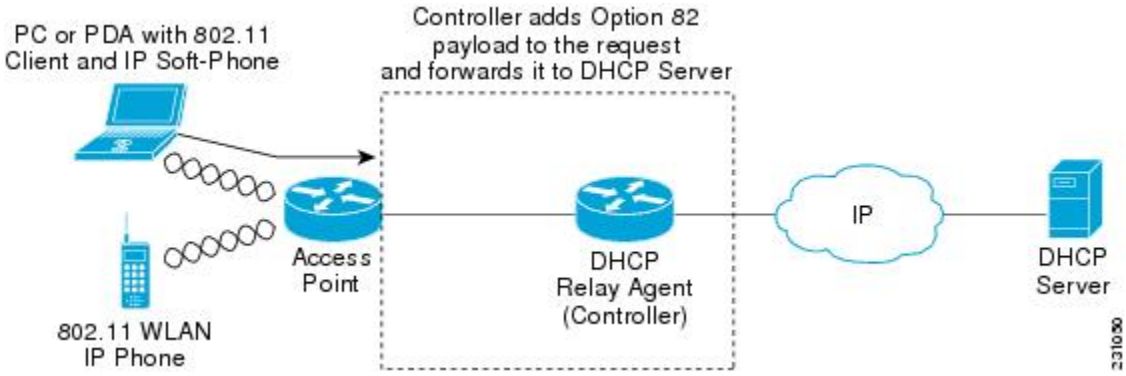
- Configure a DHCP timeout by entering this command:

  config dhcp timeout *seconds*

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 access point forwards all 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 access point, depending on how you configure this option.

Note Any 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.

This section contains the following subsections:

Restrictions on DHCP Option 82

- DHCP option 82 is not supported for use with auto-anchor mobility.

Configuring DHCP Option 82 (GUI)

Procedure

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **Enable DHCP Proxy** check box to enable DHCP proxy.

Step 3 Choose a DHCP Option 82 format from the drop-down list. You can choose either binary or ascii to specify the format of the DHCP option 82 payload.

Step 4 Choose a DHCP Option 82 Remote ID field format from the drop-down list to specify the format of the DHCP option 82 payload.

For more information about the options available, see the Controller Online Help.

Step 5 Enter the DHCP timeout value in the DHCP Timeout field. The timeout value is globally applicable. You can specify the DHCP timeout value in range from 5 to 120 seconds.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration** .

What to do next

On the controller CLI, you can enable DHCP option 82 on the dynamic interface to which the WLAN is associated by entering this command:

config interface dhcp dynamic-interface *interface-name* **option-82 enable**

Configuring DHCP Option 82 (CLI)

Procedure

- Configure the format of the DHCP option 82 payload by entering one of these commands:
  - **config dhcp opt-82 remote-id** *ap_mac*—Adds the radio MAC address of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap_mac:ssid*—Adds the radio MAC address and SSID of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap-ethmac*—Adds the Ethernet MAC address of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *apname:ssid*—Adds the AP name and SSID of the access point to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap-group-name*—Adds the AP group name to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *flex-group-name*—Adds the FlexConnect group name to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *ap-location*—Adds the AP location to the DHCP option 82 payload.
  - **config dhcp opt-82 remote-id** *apmac-vlan-id*—Adds the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.

- **config dhcp opt-82 remote-id** *apname-vlan-id*—Adds the AP name and its VLAN ID to the DHCP option 82 payload.
- **config dhcp opt-82 remote-id** *ap-ethmac-ssid*—Adds the Ethernet MAC address of the access point and the SSID to the DHCP option 82 payload.

- Configure the format of the DHCP option 82 as binary or ASCII by entering this command:

  config dhcp opt-82 format {**binary** | **ascii**}

- Enable DHCP Option 82 on the dynamic interface to which the WLAN is associated by entering this command:

  config interface dhcp dynamic-interface *interface-name* **option-82 enable**

- See the status of DHCP option 82 on the dynamic interface by entering the **show interface detailed** *dynamic-interface-name*command.

Configuring DHCP Option 82 Insertion in Bridge Mode (CLI)

Procedure

- Configure DHCP Option 82 insertion in Bridge mode on the management interface by entering this command:

  config interface dhcp management option-82 bridge-mode-insertion {**enable** | **disable**}

Note Enter the **show interface detailed management** command to see if DHCP Option 82 Bridge mode insertion is enabled or disabled on the management interface.

- Configure DHCP Option 82 insertion in Bridge mode on the dynamic interface by entering this command:

  config interface dhcp dynamic-interface *dynamic-interface-name* **option-82 bridge-mode-insertion** {**enable** | **disable**}

Note Enter the **show interface detailed** *dynamic-interface-name* command to see if DHCP Option 82 Bridge mode insertion is enabled or disabled on the dynamic interface.

DHCP Option 82 Link Select and VPN Select Suboptions

In a wireless environment, when a client requests a DHCP address, specify to the DHCP server the subnet from which the IP address has to be assigned, using the *giaddr* field in the DHCP DISCOVER packet. You can also use the giaddr field to specify the address that the DHCP server can use to communicate with the DHCP relay agent (controller). It is difficult to determine that the controller IP address in the subnet is reachable from the DHCP server. Hence, there is a need to send link-selection information that is distinct from the controller-reachable address to the DHCP server. Using the DHCP link select (DHCP option 82, suboption 5) configured on the controller interface, the link selection information distinct from controller's reachable address is sent to the DHCP server.

In a large network's wireless environment, the Cisco Network Registrar (CNR) server, which is a DHCP server, has multiple pools created based on VPN IDs or VRF names. Using these pools, you can assign IP address to a client with the help of the DHCP VPN Select option (DHCP option 82 and suboption 151). When you enable DHCP VPN Select (DHCP option 82 and suboption 151) on the controller interface, the controller sends the VPN ID or VRF name of the pool from which the IP address has to be assigned to the client. The DHCP VPN Select option enables easy-to-operate, shared usage of a centralized DHCP server, resulting in cost savings.

DHCP Link Select

Configure DHCP Link Select (DHCP option 82, suboption 5) on the management and dynamic interfaces of the controller. Before configuring DHCP Link Select on the controller interface, enable the DHCP proxy and DHCP option 82 on that interface.

When the Link Select option is enabled on the controller interface, suboption 5 is added to the packet with the IP address information that contains the desired subnet address for the corresponding client. The subnet address is the controller interface address mapped to the client VLAN interface. The DHCP server uses the subnet address to assign the IP address to the DHCP client.

DHCP VPN Select

Configure DHCP VPN Select (DHCP option 82, suboption 151) on the management and dynamic interfaces of the controller. Before configuring DHCP VPN Select on the controller interface, enable the DHCP proxy and DHCP option 82 on that interface.

You can configure different VPN IDs or VRF names on the same controller or different controllers using the VPN Select feature configured on the controller interface. Configuring the VPN Select feature, results in the DHCP server VPN pools having nonoverlapping addresses.

You must add VSS Control suboption 152 every time VSS suboption 151 is sent to the DHCP server. If the DHCP server understands and acts on VSS suboption 151, VSS Control suboption 152 is removed from the DHCP acknowledgment. If the DHCP server copies back VSS Control suboption 152 in the DHCP acknowledgment, it means that the DHCP server does not have the required support for the VSS suboption.

Mobility Considerations

Same Subnet

VPN ID or VRF name mapping to a WLAN should be the same on all the controllers in a mobility group. For example, if WLAN1 interface maps to VPN ID 1 and WLAN2 interface maps to VPN ID 2 maps on WLC A, then WLC B should also have WLAN1 interface mapping to VPN ID 1 and WLAN2 interface mapping to VPN ID 2. This way, when client L2 roams to another controller, the roamed controller's DHCP configuration will ensure that the client is assigned an address from the same VPN.

Different subnet mobility

With L3 mobility, all the DHCP DISCOVER packets are sent to the anchor and the assignment of the original VPN is ensured.

Auto anchor mobility

All the DHCP DISCOVER packets are sent to the anchor and the assignment of the original VPN is ensured.

Prerequisites for DHCP Option 82 Link Select and VPN Select

- The DHCP mode should be set to proxy.
- The DHCP external server should be configured.
- DHCP Option 82 must be enabled on the controller.
- The interface being configured should not be of type service or virtual.
- The relay source interface name should be a valid interface with IP address configured.

Note Proxy mode is not supported for IPv6.

Configuring DHCP Option 82 Link Select and VPN Select (GUI)

Procedure

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Select the interface you want to configure the DHCP option-82 link select or VPN select.

You can configure the DHCP option-82 link select on the management or dynamic interfaces in the controller.

The **Interfaces > Edit** page is displayed with DHCP information on the primary and secondary DHCP servers configured in the controller. If the primary and secondary servers are not listed, you must enter values for the IP address of the DHCP servers in the text boxes displayed in this window.

Step 3 Select the Enable DHCP Option 82 check box to enable DHCP option 82 on the interface.

Step 4 Select the Enable DHCP Option 82-Link Select check box to enable link select on the interface.

Step 5 From the Link Select relay source drop-down list, choose **management** or **dynamic** to enable link select on the interface.

When link select is enabled, you can select any interface as relay source management and dynamic interface configured on the controller.

Step 6 Select the Enable DHCP Option 82-VPN Select check box to enable VPN select on the management interface.

When VPN select is enabled, you can configure either VRF Name or VPN ID. If you try to configure both the options, you are prompted with an error message.

Step 7 In the VPN Select - VRF name text box, enter the VRF name.

Step 8 In the VPN Select - VPN ID text box, enter the VPN ID.

VPN ID should be provided in format of xxxxxx:xxxxxxxx.

Step 9 Click **Apply**.

Configuring DHCP Option 82 Link Select and VPN Select (CLI)

Procedure

Step 1 Configure the dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* { **option-82** | **primary** | **proxy-mode** }

Step 2 Configure DHCP Option 82 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82** { **enable** | **disable** | **linksel** | **vpnsel** }

Step 3 Configure Link Select suboption 5 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel** { **enable** | **disable** | **relaysrc** }
- To enable link select on the dynamic interface, first you need to enter the **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel relaysrc** command followed by the **config interface dhcp dynamic-interface** *interface-name* **option-82 linksel enable** command.

Step 4 Configure VPN Select suboption 151 on a dynamic interface using the following commands:

- **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel** { **enable** | **disable** | **vrfname** *vrf-name* | **vpnid** *vpn-id* }

  The value of *vpn-id* is denoted in the *oui:vpn-ndex* format *xxxxxx:xxxxxxxx*.

  You can configure either VPN ID or VRF name for VPN Select on the dynamic interface. If VPN ID is already configured and you try to configure VRF name, then the earlier configuration is cleared when VPN select is disabled.

  VRF name is denoted as a string of seven octets.

  To enable VPN select on a dynamic interface, first you need to enter the **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel vpnid** *vpn-id* or **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel vrfname** *vrfname* command followed by the **config interface dhcp dynamic-interface** *interface-name* **option-82 vpnsel enable** command.

Step 5 Configure Link Select suboption 5 on a management interface using the following commands:

- **config interface dhcp management option-82 linkselect** { **enable** | **disable** | **relaysrc** } *interface-name*
- To enable link select on the management interface, enter the **config interface dhcp management option-82 linkselect relaysrc** command followed by the **config interface dhcp management option-82 linkselect enable** command.

Step 6 Configure VPN Select suboption 151 on a management interface using the following commands:

- **config interface dhcp management option-82 vpnselect** { **enable** | **disable** | **vpnid** *vpn-id* | **vrfname** *vrf-name* }

  VPN ID value is denoted in the *oui:vpn-ndex* format *xxxxxx:xxxxxxxx*.

You can configure either VPN ID or VRF name for VPN select on the management interface. If VPN ID is already configured and you try to configure VRF name, then the earlier configuration is cleared when VPN select is disabled.

VRF name is denoted as a string of seven octets.

To enable VPN select on the management interface, enter the **config interface dhcp management option-82 vpnsel vpnid** *vpn-id* or **config interface dhcp management option-82 vpnselect vrfname** *vrf-name* command followed by the **config interface dhcp management option-82 vpnsel enable** command.

Step 7 Save the configuration using the following command: **save config**

Step 8 To view the details of the Link Select settings or the VPN Select interface settings, enter the following command: **show interface detailed**

Internal DHCP Server

Controllers have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in internal DHCP server that assign IP addresses and subnet masks to wireless clients. Typically, one controller can have one or more internal DHCP server that each provide a range of IP addresses.

Internal DHCP server are needed for internal DHCP to work. Once DHCP is defined on the controller, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the controller's management interface.

Note The controller has the ability to provide internal DHCP server. This feature is very limited and considered as convenience that is often used simple demonstration or proof-of-concept, for example in a lab environment. The best practice is NOT to use this feature in an enterprise production network.

Read more about this at: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html#anc16

Per WLAN DHCP Servers

By default, when using DHCP proxy mode, a WLAN's clients use the DHCP servers that are configured on the mapped interfaces. You can override the interface's DHCP servers by configuring per-WLAN DHCP servers.

This section contains the following subsections:

Restrictions for Configuring Internal DHCP Server

- You can configure up to 16 Internal DHCP scopes.
- Internal DHCP Server is not supported on the following controllers:
  - Cisco 5520 Wireless Controller

- Cisco 8540 Wireless Controller
- Cisco Virtual Wireless Controller

- You must configure DHCP Proxy Mode to use the Internal DHCP Server.
- 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.

Configuring DHCP Scopes (GUI)

Procedure

Step 1 Choose **Controller** > **Internal DHCP Server** > **DHCP Scope** to open the **DHCP Scopes** page.

This page lists any DHCP scopes that have already been configured.

Note
If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose **Remove**.

Step 2 Click **New** to add a new DHCP scope. The **DHCP Scope > New** page appears.

Step 3 In the **Scope Name** field, enter a name for the new DHCP scope.

Step 4 Click **Apply**. When the **DHCP Scopes** page reappears, click the name of the new scope. The **DHCP Scope > Edit** page appears.

Step 5 In the **Pool Start Address** field, enter the starting IP address in the range assigned to the clients.

Note
This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 6 In the **Pool End Address** field, enter the ending IP address in the range assigned to the clients.

Note
This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 7 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 on the **Interfaces** page.

Step 8 In the **Netmask** field, enter the subnet mask assigned to all wireless clients.

Step 9 In the **Lease Time** field, enter the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client.

Step 10 In the **Default Routers** field, enter the IP address of the optional router connecting the controllers. Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 11 In the **DNS Domain Name** field, enter the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers.

Step 12 In the **DNS Servers** field, enter the IP address of the optional DNS server. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 13 In the **Netbios Name Servers** field, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server.

Step 14 From the **Status** drop-down list, choose **Enabled** to enable this DHCP scope or choose **Disabled** to disable it.

Step 15 Save the configuration.

Step 16 Choose **DHCP Allocated Leases** to see the remaining lease time for wireless clients. The DHCP Allocated Lease page appears, showing the MAC address, IP address, and remaining lease time for the wireless clients.

Configuring DHCP Scopes (CLI)

Procedure

Step 1 Create a new DHCP scope by entering this command:

config dhcp create-scope scope

Note
If you ever want to delete a DHCP scope, enter this command: **config dhcp delete-scope scope**.

Step 2 Specify the starting and ending IP address in the range assigned to the clients by entering this command:

config dhcp address-pool *scope start end*

Note
This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 3 Specify the network served by this DHCP scope (the IP address used by the management interface with the Netmask applied) and the subnet mask assigned to all wireless clients by entering this command:

config dhcp network *scope network netmask*

Step 4 Specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client by entering this command:

config dhcp lease *scope lease_duration*

Step 5 Specify the IP address of the optional router connecting the controllers by entering this command:

config dhcp default-router *scope router_1* [*router_2*] [*router_3*]

Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 6 Specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers by entering this command:

config dhcp domain *scope domain*

Step 7 Specify the IP address of the optional DNS server(s) by entering this command:

config dhcp dns-servers scope *dns1* [*dns2*] [*dns3*]

Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope

Step 8 Specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server by entering this command:

config dhcp netbios-name-server *scope wins1* [*wins2*] [*wins3*]

Step 9 Enable or disable this DHCP scope by entering this command:

config dhcp {**enable** | **disable**} *scope*

Step 10 Save your changes by entering this command:

save config

Step 11 See the list of configured DHCP scopes by entering this command:

show dhcp summary

Information similar to the following appears:

```
Scope Name     Enabled      Address Range
Scope 1         No        0.0.0.0 -> 0.0.0.0
Scope 2         No        0.0.0.0 -> 0.0.0.0
```

Step 12 Display the DHCP information for a particular scope by entering this command:

show dhcp *scope*

Information similar to the following appears:

```
Enabled..........................  No
Lease Time.......................  0
Pool Start.......................  0.0.0.0
Pool End.........................  0.0.0.0
Network..........................  0.0.0.0
Netmask..........................  0.0.0.0
Default Routers..................  0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.......................
DNS..............................  0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers.............  0.0.0.0 0.0.0.0 0.0.0.0
```

Configuring DHCP Per WLAN (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.

Procedure

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, uncheck 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, check the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** field. 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.

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, check 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, check the **Status** check box and click **Apply** to reenable the WLAN.

Step 11 Click **Save Configuration**.

Configuring DHCP Per WLAN (CLI)

Procedure

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* [**required**]

The **required** is an optional argument. Using this argument forces DHCP address assignment to be applied to the WLAN.

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*

DHCP Release Override on Cisco APs

If you are using Microsoft Windows Server 2008 R2 or 2012 as the DHCP server and after an AP or a controller reboot, the AP might fail to associate with the controller because of no valid IP address. This can be caused due to an interoperability issue with the Microsoft server.

When a controller is rebooted, the AP tries to associate with the controller. During this time, the AP keeps renewing the IP address. Every time the AP releases the current DHCP lease, the AP sends out 3 DHCP release packets. This functionality of sending 3 DHCP release packets is common across all Cisco IOS software-based products. Cisco DHCP servers running on various Cisco devices release the IP address when they get the first DHCP release message but ignore the later messages. However, the Microsoft DHCP server marks the AP as BAD_ADDRESS when it receives the second and the third DHCP release packets.

A workaround for this issue is to configure DHCP release override and set the number of DHCP releases sent by AP to 1, on a Cisco AP or all APs by entering this command:

config ap dhcp release-override enable {*cisco-ap* | **all**}

Note We recommend that you use this configuration only in highly reliable networks.

For more information about this issue, see the CSCuv61271 caveat.

Debugging DHCP (CLI)

Use these commands to debug DHCP:

- **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.