Configuring Policy Profile Features

- Configure AAA override (CLI), on page 1
- Configure override VLAN for central switching (CLI), on page 2
- Configure override VLAN for local switching (CLI), on page 3
- VLAN override verification on Layer 3 web authentication, on page 4
- Configuring DHCP for WLANS (CLI), on page 4
- Configuring DHCP for WLANs (GUI), on page 17

Configure AAA override (CLI)

Enable AAA override functionality to allow authentication servers to dynamically override wireless policy configurations on a per-client basis.

AAA override allows RADIUS servers to push policy attributes that supersede the locally configured wireless policy settings. This is useful for implementing dynamic policies based on user authentication results.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile and enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Example:

```
Device(config)# wireless profile policy test-wgb
```

Step 3 Configure AAA policy override.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Note
If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server.

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

AAA override is now enabled for the wireless policy profile, allowing RADIUS server attributes to override local policy settings for authenticated clients.

Configure override VLAN for central switching (CLI)

Enable dynamic VLAN assignment from a RADIUS server for centrally switched wireless clients.

Override VLAN configuration allows the RADIUS server to dynamically assign VLANs to wireless clients during authentication, providing flexible network segmentation based on user credentials or policies.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Define VLANs that can be pushed from the RADIUS server.

Example:

```
Device(config)# vlan vlan-id
```

Example:

```
Device(config)# vlan 20
```

The valid VLAN ID range is 1 to 4094.

Step 3 (Optional) Change the default name of the VLAN.

Example:

```
Device(config-vlan)# name vlan-name
```

Example:

```
Device(config-vlan)# name vlan_ascii
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-vlan)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The override VLAN is configured and ready to accept dynamic VLAN assignments from the RADIUS server for centrally switched clients.

Configure override VLAN for local switching (CLI)

Configure VLAN name to ID mapping under flex profile for local switching scenarios.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a Flex profile.

Example:

```
Device(config)# wireless profile flex flex-profile-name
```

Example:

```
Device(config)# wireless profile flex rr-xyz-flex-profile
```

Step 3 Define VLANs that can be pushed from the RADIUS server.

Example:

```
Device(config-wireless-flex-profile)# vlan-name vlan-name
```

Example:

```
Device(config-wireless-flex-profile)# vlan-name vlan_123
```

Step 4 Configure VLAN ID.

Example:

```
Device(config-wireless-flex-profile-vlan)# vlan-id vlan-id
```

Example:

```
Device(config-wireless-flex-profile-vlan)# vlan-id 23
```

The valid VLAN ID range is 1 to 4096.

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-flex-profile-vlan)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The override VLAN is now configured for local switching with the specified flex profile, enabling VLAN name to ID mapping for wireless clients.

VLAN override verification on Layer 3 web authentication

Verify VLAN override on layer 3 web authentication using specific show commands to display override status and statistics.

To display the VLAN override after L3 authentication, use this command:

```
Device# show wireless client mac <mac> detail
[…]
        Vlan Override after L3 Auth: True
```

To display the statistics about client, use this command:

```
Device# show wireless stats client detail
[…]
      Total L3 VLAN Override vlan change received      : 1
      Total L3 VLAN Override disassociations sent      : 1
      Total L3 VLAN Override re-associations received  : 1
      Total L3 VLAN Override successful VLAN change    : 1
      […]
      L3 VLAN Override connection timeout                          : 0
```

Configuring DHCP for WLANS (CLI)

Configuring DHCP Scopes (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp pool** *pool-name* **Example:** `(config)#ip dhcp pool test-pool`	Configures the DHCP pool address.

	Command or Action	Purpose
Step 3	**network** *network-name mask-address* **Example:** `(dhcp-config)#network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `(dhcp-config)#dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configure the internal DHCP server under client VLAN SVI (CLI)

Set up an internal DHCP server to provide IP address assignment for wireless and wired clients through the client VLAN SVI configuration.

The internal DHCP server can be configured under the client VLAN SVI to serve both wireless and wired clients. This configuration requires proper IP addressing and helper configuration to function correctly with the wireless infrastructure.

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

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a loopback interface and enter interface configuration mode.

Example:

```
Device(config)# interface loopback interface-number
```

Example:

```
Device(config)# interface Loopback0
```

Step 3 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 10.10.10.1 255.255.255.255
```

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 5 Configure the VLAN ID.

Example:

```
Device(config)# interface vlan vlan-id
```

Example:

```
Device(config)# interface vlan 32
```

Step 6 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 192.168.32.100 255.255.255.0
```

Step 7 Configure the destination address for UDP broadcasts.

Example:

```
Device(config-if)# ip helper-address ip-address
```

Example:

```
Device(config-if)# ip helper-address 10.10.10.1
```

Note
If the IP address used in the **IP helper-address** command is an internal address of the controller an internal DHCP server is used. Otherwise, the external DHCP server is used.

Step 8 Disable the Maintenance Operation Protocol (MOP) for an interface.

Example:

```
Device(config-if)# no mop enabled
```

Step 9 Disable the task of sending MOP periodic system ID messages.

Example:

```
Device(config-if)# no mop sysid
```

Step 10 Exit interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 11 Specify the IP address that the DHCP server should not assign to DHCP clients.

Example:

```
Device(config)# ip dhcp excluded-address ip-address
```

Example:

```
Device(config)# ip dhcp excluded-address 192.168.32.1
```

Step 12 Specify the IP addresses that the DHCP server should not assign to DHCP clients.

Example:

```
Device(config)# ip dhcp excluded-address ip-address
```

Example:

```
Device(config)# ip dhcp excluded-address 192.168.32.100
```

Step 13 Configure the DHCP pool address.

Example:

```
Device(config)# ip dhcp pool pool-name
```

Example:

```
Device(config)# ip dhcp pool pool-vlan32
```

Step 14 Specify the network number in dotted-decimal notation, along with the mask address.

Example:

```
Device(dhcp-config)# network network-address subnet-mask
```

Example:

```
Device(dhcp-config)# network 192.168.32.0 255.255.255.0
```

Step 15 Specify the IP address of the default router for a DHCP client.

Example:

```
Device(dhcp-config)# default-router ip-address
```

Example:

```
Device(dhcp-config)# default-router 192.168.32.1
```

Step 16 Exit DHCP configuration mode.

Example:

```
Device(dhcp-config)# exit
```

Step 17 Configure the WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Example:

```
Device(config)# wireless profile policy default-policy-profile
```

Step 18 Configure central association for locally switched clients.

Example:

```
Device(config-wireless-policy)# central association
```

Step 19 Configure the central DHCP for locally switched clients.

Example:

```
Device(config-wireless-policy)# central dhcp
```

Step 20 Configure WLAN for central switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 21 Add a description for the policy profile.

Example:

```
Device(config-wireless-policy)# description "policy-profile-description"
```

Example:

```
Device(config-wireless-policy)# description "default policy profile"
```

Step 22 Assign the profile policy to the VLAN.

Example:

```
Device(config-wireless-policy)# vlan vlan-id
```

Example:

```
Device(config-wireless-policy)# vlan 32
```

Step 23 Enable the wireless profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The internal DHCP server is now configured under the client VLAN SVI and can provide IP address assignment to both wireless and wired clients connected to the specified VLAN.

Configure the internal DHCP server under a wireless policy profile (CLI)

Enable DHCP services for wireless clients by configuring an internal DHCP server within a wireless policy profile.

The internal DHCP server provides IP address assignment and network configuration to wireless clients. This configuration includes setting up loopback and VLAN interfaces, defining DHCP pools, and associating the DHCP server with a wireless policy profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a loopback interface and enter interface configuration mode.

Example:

```
Device(config)# interface loopback interface-number
```

Example:

```
Device(config)# interface Loopback0
```

Step 3 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 10.10.10.1 255.255.255.255
```

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 5 Configure the VLAN ID.

Example:

```
Device(config)# interface vlan vlan-id
```

Example:

```
Device(config)# interface vlan 32
```

Step 6 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 192.168.32.100 255.255.255.0
```

Step 7 Disable the Maintenance Operation Protocol (MOP) for an interface.

Example:

```
Device(config-if)# no mop enabled
```

Step 8 Disable the task of sending MOP periodic system ID messages.

Example:

```
Device(config-if)# no mop sysid
```

Step 9 Exit interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 10 Specify the IP address that the DHCP server should not assign to DHCP clients.

Example:

```
Device(config)# ip dhcp excluded-address ip-address
```

Example:

```
Device(config)# ip dhcp excluded-address 192.168.32.100
```

Step 11 Configure the DHCP pool address.

Example:

```
Device(config)# ip dhcp pool pool-name
```

Example:

```
Device(config)# ip dhcp pool pool-vlan32
```

Step 12 Specify the network number in dotted-decimal notation along with the mask address.

Example:

```
Device(dhcp-config)# network network-address subnet-mask
```

Example:

```
Device(dhcp-config)# network 192.168.32.0 255.255.255.0
```

Step 13 Specify the IP address of the default router for a DHCP client.

Example:

```
Device(dhcp-config)# default-router ip-address
```

Example:

```
Device(dhcp-config)# default-router 192.168.32.1
```

Step 14 Exit DHCP configuration mode.

Example:

```
Device(dhcp-config)# exit
```

Step 15 Configure a WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Example:

```
Device(config)# wireless profile policy default-policy-profile
```

Step 16 Configure central association for locally switched clients.

Example:

```
Device(config-wireless-policy)# central association
```

Step 17 Configure local switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 18 Add a description for the policy profile.

Example:

```
Device(config-wireless-policy)# description "policy-profile-name"
```

Example:

```
Device(config-wireless-policy)# description "default policy profile"
```

Step 19 Enable DHCP Option 82 for the wireless clients.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82
```

Step 20 Enable ASCII on DHCP Option 82.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82 ascii
```

Step 21 Enable VLAN ID.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan-id
```

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32
```

Step 22 Support the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82 rid
```

Step 23 Configure the WLAN's IPv4 DHCP server.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp server ip-address
```

Example:

```
Device(config-wireless-policy)# ipv4 dhcp server 10.10.10.1
```

Step 24 Assign the profile policy to the VLAN.

Example:

```
Device(config-wireless-policy)# vlan vlan-id
```

Example:

```
Device(config-wireless-policy)# vlan 32
```

Step 25 Enable the wireless profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The internal DHCP server is now configured and operational within the wireless policy profile, ready to provide IP addresses and network configuration to wireless clients.

Configure the internal DHCP server globally (CLI)

Enable centralized DHCP services for wireless clients by configuring the internal DHCP server with appropriate network pools and policies.

The internal DHCP server configuration allows the wireless controller to provide IP addresses to wireless clients directly, eliminating the need for external DHCP servers in certain network deployments.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a loopback interface and enter interface configuration mode.

Example:

```
Device(config)# interface loopback interface-number
```

Example:

```
Device(config)# interface Loopback0
```

Step 3 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 10.10.10.1 255.255.255.255
```

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 5 Configure the VLAN ID.

Example:

```
Device(config)# interface vlan vlan-id
```

Example:

```
Device(config)# interface vlan 32
```

Step 6 Configure the IP address for the interface.

Example:

```
Device(config-if)# ip address ip-address subnet-mask
```

Example:

```
Device(config-if)# ip address 192.168.32.100 255.255.255.0
```

Step 7 Disable the Maintenance Operation Protocol (MOP) for an interface.

Example:

```
Device(config-if)# no mop enabled
```

Step 8 Disable the task of sending the MOP periodic system ID messages.

Example:

```
Device(config-if)# no mop sysid
```

Step 9 Exit the interface configuration mode.

Example:

```
Device(config-if)# exit
```

Step 10 Specify the target DHCP server parameters.

Example:

```
Device(config)# ip dhcp-server ip-address
```

Example:

```
Device(config)# ip dhcp-server 10.10.10.1
```

Step 11 Specify the IP address that the DHCP server should not assign to DHCP clients.

Example:

```
Device(config)# ip dhcp excluded-address ip-address
```

Example:

```
Device(config)# ip dhcp excluded-address 192.168.32.100
```

Step 12 Configure the DHCP pool address.

Example:

```
Device(config)# ip dhcp pool pool-name
```

Example:

```
Device(config)# ip dhcp pool pool-vlan32
```

Step 13 Specify the network number in dotted-decimal notation along with the mask address.

Example:

```
Device(dhcp-config)# network network-address subnet-mask
```

Example:

```
Device(dhcp-config)# network 192.168.32.0 255.255.255.0
```

Step 14 Specify the IP address of the default router for a DHCP client.

Example:

```
Device(dhcp-config)# default-router ip-address
```

Example:

```
Device(dhcp-config)# default-router 192.168.32.1
```

Step 15 Exit DHCP configuration mode.

Example:

```
Device(dhcp-config)# exit
```

Step 16 Configure a WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Example:

```
Device(config)# wireless profile policy default-policy-profile
```

Step 17 Configure central association for locally switched clients.

Example:

```
Device(config-wireless-policy)# central association
```

Step 18 Configure central DHCP for locally switched clients.

Example:

```
Device(config-wireless-policy)# central dhcp
```

Step 19 Configure local switching.

Example:

```
Device(config-wireless-policy)# central switching
```

Step 20 Add a description for the policy profile.

Example:

```
Device(config-wireless-policy)# description policy-profile-description
```

Example:

```
Device(config-wireless-policy)# description "default policy profile"
```

Step 21 Assign the profile policy to the VLAN.

Example:

```
Device(config-wireless-policy)# vlan vlan-id
```

Example:

```
Device(config-wireless-policy)# vlan 32
```

Step 22 Enable the profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The internal DHCP server is now configured globally with the specified pool, exclusions, and wireless policy profile settings to serve DHCP requests from wireless clients.

Verify internal DHCP configuration

Verify internal DHCP configuration using specific show commands to check client binding, DHCP relay statistics for wireless clients, and DHCP packet punt statistics.

Client binding verification

To verify client binding, use this 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
```

DHCP relay statistics verification

To verify the DHCP relay statistics for a wireless client, use this 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
```

DHCP packet punt statistics verification

To verify the DHCP packet punt statistics in CPP, use this 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
```

Configure FlexConnect DHCP-required (CLI)

Enable the FlexConnect DHCP-required feature to ensure clients obtain IP addresses through DHCP before being allowed network access.

FlexConnect DHCP-required forces clients to obtain an IP address through DHCP before they can communicate on the network. This configuration is performed through the CLI on a WLAN policy profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile and enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Example:

```
Device(config)# wireless profile policy rr-xyz-policy-1
```

Step 3 Enable the FlexConnect DHCP-Required feature.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp required
```

Step 4 Save the configuration.

Example:

```
Device(config-wireless-policy)# no shutdown
```

FlexConnect DHCP-required is now configured on the policy profile, requiring clients to obtain IP addresses through DHCP before network access is granted.

Verify FlexConnect DHCP-required

Verify FlexConnect DHCP-required functionality using wireless client commands to confirm IP address learning and client states.

- 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
```

Configuring DHCP for WLANs (GUI)

Configure DHCP scopes (GUI)

Configure DHCP scopes to automatically assign IP addresses and network configuration parameters to wireless clients on your network.

DHCP scopes define the range of IP addresses available for assignment to clients, along with associated network configuration parameters such as subnet masks, default routers, and DNS servers.

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**.

The DHCP scope is configured and ready to assign IP addresses and network configuration parameters to wireless clients.

Configure the internal DHCP server under client VLAN SVI (GUI)

This task configures the internal DHCP server settings for a client VLAN Switched Virtual Interface (SVI) to enable DHCP relay functionality.

Use this procedure when you need to set up DHCP relay on an SVI to forward DHCP requests to a designated helper address. This configuration is typically performed on network switches to enable DHCP services across VLANs.

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**.

The internal DHCP server is configured under the client VLAN SVI with the specified helper address, enabling DHCP relay functionality for the selected SVI.

Configure the internal DHCP server under a wireless policy profile (GUI)

Configure DHCP settings to enable automatic IP address assignment for wireless clients connected to the network under a specific policy profile.

Use this procedure when you need to set up internal DHCP server functionality within a wireless policy profile to provide IP address allocation for connected wireless devices.

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**.

The internal DHCP server is configured under the wireless policy profile and the settings are applied to the device.

Configure the internal DHCP server globally (GUI)

Configure a DHCP pool to enable automatic IP address assignment for network devices through the internal DHCP server.

Use this procedure when you need to set up centralized IP address management for your network infrastructure using the GUI interface.

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**.

The DHCP pool is created and applied to the device, enabling automatic IP address assignment within the specified range.

Configure FlexConnect DHCP-Required (GUI)

This task enables the FlexConnect DHCP-Required feature through the GUI interface to ensure proper DHCP configuration for FlexConnect access points.

Use this procedure when you need to configure the FlexConnect DHCP-Required feature through the GUI interface for policy profiles.

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**.

The FlexConnect DHCP-Required feature is now enabled for the selected policy profile, and the configuration is applied to the associated devices.