Configuring FlexConnect

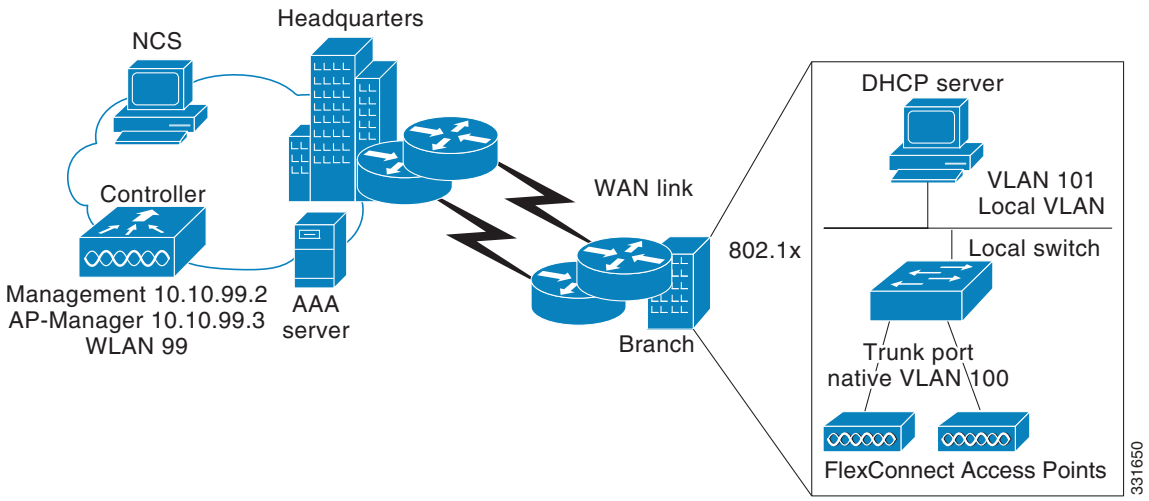
This chapter describes contains the following sections:

Information About FlexConnect

FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 16-1 shows a typical FlexConnect deployment.

Figure 16-1 FlexConnect Deployment



This section contains the following topics:

FlexConnect Authentication Process

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

Note Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode. This can be done using the GUI or CLI.

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

  Note OTAP is no longer supported on the controllers with 6.0.196 code and above.

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

Note For more information about how access points find controllers, see Chapter 9, "Controlling Lightweight Access Points," or the controller deployment guide at: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html

When a FlexConnect access point can reach the controller (referred to as the *connected mode*), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode and authenticates clients by itself.

Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.
- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

  In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

  - Policy type
  - Access VLAN
  - VLAN name
  - Supported rates
  - Encryption cipher

  Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

Note Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

Notes about local authentication are as follows:

- Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.

  - Local RADIUS on the controller is not supported.
  - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
  - Local authentication in connected mode requires a WLAN configuration.

Note When locally switched clients that are connected to a FlexConnect access point renew the IP addresses, on joining back, the client continues to stay in the run state. These clients are not reauthenticated by the controller.

- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.
- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the "local authentication, local switching" state and continue new client authentications. In controller software release 4.2 or later releases, this configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or CCKM, but these authentication types require that an external RADIUS server be configured. You can also configure a local RADIUS server on a FlexConnect access point to support 802.1X in a standalone mode or with local authentication.

Other WLANs enter either the "authentication down, switching down" state (if the WLAN was configured for central switching) or the "authentication down, local switching" state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the **config radius auth add** CLI command (unless the server order is overridden for a particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

Note A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When a FlexConnect access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For web-authentication WLANs, existing clients are not disassociated, but the FlexConnect access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to web-authentication WLANs. Controller-dependent activities, such as network access control (NAC) and web authentication (guest access), are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller. Most radio resource management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a FlexConnect access point supports dynamic frequency selection in standalone mode.

Note

- For Wi-Fi Protected Access version 2 (WPA2) in FlexConnect standalone mode or local-auth in connected mode or cckm fast-roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or cckm fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and CCKM fast-roaming in connected mode.

Note If your controller is configured for NAC, clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the "Configuring Dynamic Interfaces" section on page 4-15 for information on creating quarantined VLANs and the "Configuring NAC Out-of-Band Integration" section on page 8-70 for information on configuring NAC out-of-band support.

Note Even after configuring WLAN Override to stop transmitting locally switched WLAN on both radios, the WLAN still appears in the H-REAP VLAN mapping configuration on the AP.

When a FlexConnect access point enters into a standalone mode, the following occurs:

- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:

- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

Guidelines and Limitations

- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to four fragmented packets or a minimum 500-byte maximum transmission unit (MTU) WAN link.
- FlexConnect is supported only on the following access points: Cisco Aironet 1130AG, 1140, 1240, 1250, 1260, AP801, AP802 and Cisco Aironet 600 Series OfficeExtend Access Points.

- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In cases where you cannot achieve the 300 milliseconds round-trip latency, you can configure the access point to perform local authentication.
- Starting with the 7.0.116.0 release, the controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all clients are disconnected and are authenticated again. In the controller software 7.0.116.0 and later releases, this functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity.

  This feature can be used only when both the access point and the controller have the same configuration.
- Clients that are centrally authenticated are reauthenticated.
- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode. After the access point moves from the standalone mode to the connected mode, the access point's radio is also reset.
- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and secondary or backup controller must be the same.
- Session timeout and reauthentication is performed when the access point establishes a connected to the controller.
- After the client connection has been established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default values only after the session timer expires.
- There is no deployment restriction on the number of FlexConnect access points per location. However, the minimum bandwidth restriction remains 128 kbps with the roundtrip latency no greater than 300 ms and the maximum transmission unit (MTU) no smaller than 500 bytes.
- A newly connected access point cannot be booted in FlexConnect mode.
- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In FlexConnect mode, the access point can receive multicast packets only in unicast form.
- To use CCKM fast roaming with FlexConnect access points, you must configure FlexConnect Groups.
- FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points also support a many-to-one NAT/PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

  Note Although NAT and PAT are supported for FlexConnect access points, they are not supported on the corresponding controller. Cisco does not support configurations in which the controller is behind a NAT/PAT boundary.

- VPN and PPTP are supported for locally switched traffic if these security types are accessible locally at the access point.

- FlexConnect access points support multiple SSIDs. See the "Creating WLANs" section on page 8-3 for more information.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching. See the "Configuring NAC Out-of-Band Integration" section on page 8-70 for more information.
- The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features (such as WLAN overrides, VLANs, static channel number, and so on) might not operate correctly. In addition, make sure to duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- The QoS profile per-user bandwidth contracts are not supported for FlexConnect locally switched WLANs. The QoS per-user bandwidth contracts are only supported for centrally switched WLANs and APs in the local mode.
- Guest user configuration is not supported with FlexConnect local switching.
- Do not connect access points in FlexConnect mode directly to a Cisco 2500 Series Controllers.
- FlexConnect access points do not support client load balancing.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at time of initialization, few syslog packets from the access point are tagged with VLAN ID 1. This is a known issue.
- FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to the IPv4 operation. FlexConnect supports client mobility for a group of up to 50 Access Points.
- FlexConnect does not support IPv6 ACLs, neighbor discovery caching, and DHCPv6 snooping of IPv6 NDP packets.
- FlexConnect does not display any IPv6 client addresses within the client detail page.
- FlexConnect Access Points with Locally Switched WLAN cannot perform IP Source Guard and prevent ARP spoofing. For Centrally Switched WLAN, the wireless controller performs the IP Source Guard and ARP Spoofing.
- To prevent ARP spoofing attacks in FlexConnect AP with Local Switching, we recommend you to use ARP Inspection.

Configuring FlexConnect

This section contains the following topics:

Note You must perform the procedures in the order listed.

Configuring the Switch at the Remote Site

Step 1 Attach the access point that will be enabled for FlexConnect to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 See the sample configuration in this procedure to configure the switch to support the FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The text in bold below shows these settings.

A sample local switch configuration is as follows:

```
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.200.228 255.255.255.224
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
 ip helper-address 209.165.201.227
!
interface Vlan101
 ip address 209.165.200.226 255.255.255.229
 ip helper-address 209.165.202.228
end
!
```

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN

- Locally switched WLAN

Configuring the Controller for FlexConnect (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the WLANs > New page.

Figure 16-2 WLANs > New Page

Step 3 From the Type drop-down list, choose **WLAN**.

Step 4 In the Profile Name text box, enter a unique profile name for the WLAN.

Step 5 In the WLAN SSID text box, enter a name for the WLAN.

Step 6 From the WLAN ID drop-down list, choose the ID number for this WLAN.

Step 7 Click **Apply** to commit your changes. The WLANs > Edit page appears.

Step 8 You can configure the controller for FlexConnect in both centrally switched and locally switched WLANs:

- To configure the controller for FlexConnect in a centrally switched WLAN:
  a. In the General tab, choose the **Status** check box to enable the WLAN.
  b. If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
  c. In the Security > Layer 2 tab, choose **WPA+WPA2** from the Layer 2 Security drop-down list and then set the WPA+WPA2 parameters as required.
- To configure the controller for FlexConnect in a locally switched WLAN:
  a. In the General tab, select the **Status** check box to enable the WLAN.
  b. If you have enabled NAC and have created a quarantined VLAN and want to use it for this WLAN, select the interface from the Interface/Interface Group(G) drop-down list in the General tab.
  c. In the Security > Layer 2 tab, select **WPA+WPA2** from the **Layer 2 Security** drop-down list and then set the WPA+WPA2 parameters as required.
  d. In the Advanced tab, select the **FlexConnect Local Switching** check box to enable local switching for the WLAN.

Note When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

Note When you enable FlexConnect local switching, the controller is enabled to learn the client's IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client's IP address, and the controller periodically drops the client. Disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client's IP address. The ability to disable this option is supported only with FlexConnect local switching; it is not supported with FlexConnect central switching.

Note For FlexConnect access points, the interface mapping at the controller for WLANs that is configured for FlexConnect local switching is inherited at the access point as the default VLAN tagging. This mapping can be changed per SSID and per FlexConnect access point. Non-FlexConnect access points tunnel all traffic back to the controller, and VLAN tagging is determined by each WLAN's interface mapping.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Example Configuration of Controller for FlexConnect

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. Table 16-1 shows three WLAN scenarios.

Table 16-1 WANs Example

WLAN	Security	Authentication	Switching	Interface Mapping (VLAN)
employee	WPA1+WPA2	Central	Central	management (centrally switched VLAN)
employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched VLAN)
guest-central	Web authentication	Central	Central	management (centrally switched VLAN)
employee-local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Note Guest user configuration is not supported with FlexConnect local switching.

Configuring the Controller for FlexConnect—For a Centrally Switched WLAN Used for Guest Access

Before you begin, you must have created guest user accounts. For more information about creating guest user accounts, see Chapter 12, "Managing User Accounts."

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 From the drop-down list, choose **Create New** and click **Go** to open the WLANs > New page.

Step 3 From the Type drop-down list, choose **WLAN**.

Step 4 In the Profile Name text box, enter **guest-central** (as per the example in Table 16-1).

Step 5 In the WLAN SSID text box, enter **guest-central**.

Step 6 From the WLAN ID drop-down list, choose and ID for the WLAN.

Step 7 Click **Apply** to commit your changes. The WLANs > Edit page appears.

Step 8 In the General tab, select the **Status** check box to enable the WLAN.

Step 9 In the Security > Layer 2 tab, choose **None** from the **Layer 2 Security** drop-down list.

Step 10 In the Security > Layer 3 tab:

a. Choose **None** from the **Layer 3 Security** drop-down list.

b. Select the **Web Policy** check box.

c. Choose **Authentication**.

Note If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL on the Layer 3 tab. For more information about ACLs, see Chapter 7, "Configuring Security Solutions."

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Note For more information about adding a local user to a WLAN and to customize the content and appearance of the login page for guest users when they access the WLAN, follow the instructions in Chapter 7, "Configuring Security Solutions.".

Configuring the Controller for FlexConnect (CLI)

- **config wlan flexconnect local-switching** *wlan_id* **enable**—Configures the WLAN for local switching.

  Note When you enable FlexConnect local switching, the controller waits to learn the client IP address by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Use the **config wlan flexconnect learn-ipaddr** *wlan_id* **disable** command to disable the client IP address learning feature so that the controller maintains the client connection without waiting to learn the client's IP address. The ability to disable this feature is supported only with FlexConnect local switching; it is not supported with FlexConnect central switching. To enable this feature, enter the **config wlan flexconnect learn-ipaddr** *wlan_id* **enable** command.

- **config wlan flexconnect local-switching** *wlan_id* **disable**—Configures the WLAN for central switching. This is the default value.

Commands Related to Configuring the Controller for FlexConnect

Use these commands to get FlexConnect information:

- **show ap config general** *Cisco_AP*—Shows VLAN configurations.
- **show wlan** *wlan_id*—Shows whether the WLAN is locally or centrally switched.
- **show client detail** *client_mac*—Shows whether the client is locally or centrally switched.

Use these commands to obtain debug information:

- **debug flexconnect aaa {event | error} {enable | disable}**—Enables or disables debugging of FlexConnect backup RADIUS server events or errors.
- **debug flexconnect cckm** {**enable | disable**}—Enables or disables debugging of FlexConnect CCKM.
- **debug flexconnect** {**enable | disable**}—Enables or disables debugging of FlexConnect Groups.
- **debug pem state** {**enable | disable**}—Enables or disables debugging of the policy manager state machine.
- **debug pem events** {**enable | disable**}—Enables or disables debugging of policy manager events.

Configuring an Access Point for FlexConnect

This section contains the following topics:

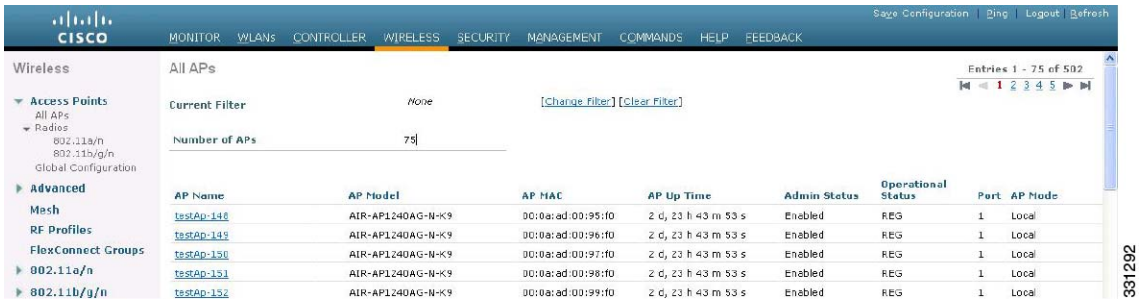
Configuring an Access Point for FlexConnect (GUI)

Ensure that the access point has been physically added to your network.

Step 1 Choose **Wireless** to open the All APs page.

Step 2 Click the name of the desired access point. The All APs > Details page appears.

Figure 16-3 All APs Page



Step 3 Choose FlexConnect from the AP Mode drop-down list to enable FlexConnect for this access point.

Note The last parameter in the Inventory tab indicates whether the access point can be configured for FlexConnect.

Step 4 Click **Apply** to commit your changes and to cause the access point to reboot.

Step 5 Choose the FlexConnect tab to open the All APs > Details for (FlexConnect) page.

If the access point belongs to a FlexConnect group, the name of the group appears in the FlexConnect Name text box.

Step 6 Select the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the Native VLAN ID text box.

Note By default, a VLAN is not enabled on the FlexConnect access point. After FlexConnect is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller.

Note To preserve the VLAN mappings in the access point after an upgrade or downgrade, it is necessary that the access point join is restricted to the controller for which it is primed. That is, no other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers which have different VLAN mappings, the VLAN mappings at the access point may get mismatched.

Step 7 Click **Apply** to commit your changes. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 8 Click the name of the same access point and then select the FlexConnect tab.

Step 9 Click **VLAN Mappings** to open the All APs > *Access Point Name* > VLAN Mappings page.

Step 10 Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the VLAN ID text box.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Note Repeat this procedure for any additional access points that need to be configured for FlexConnect at the remote site.

Configuring an Access Point for FlexConnect (CLI)

- **config ap mode flexconnect** *Cisco_AP*—Enables FlexConnect for this access point.
- **config ap flexconnect radius auth set** {**primary** | **secondary**} *ip_address auth_port secret Cisco_AP*—Configures a primary or secondary RADIUS server for a specific FlexConnect access point.

Note Only the Session Timeout RADIUS attribute is supported in standalone mode. All other attributes as well as RADIUS accounting are not supported.

Note To delete a RADIUS server that is configured for a FlexConnect access point, enter the **config ap flexconnect radius auth delete** {**primary** | **secondary**} *Cisco_AP command.*

- **config ap flexconnect vlan wlan** *wlan_id vlan-id Cisco_AP***—**Enables you to assign a VLAN ID to this FlexConnect access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap flexconnect vlan** {**enable** | **disable**} *Cisco_AP*—Enables or disables VLAN tagging for this FlexConnect access point. By default, VLAN tagging is not enabled. Once VLAN tagging is enabled on the FlexConnect access point, WLANs enabled for local switching inherit the VLAN assigned at the controller.
- **config ap flexconnect vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this FlexConnect access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per FlexConnect access point (when VLAN tagging is enabled). Make sure the switch port to which the access point is connected has a corresponding native VLAN configured as well. If the FlexConnect access point's native VLAN setting and the upstream switchport native VLAN do not match, the access point cannot transmit packets to and from the controller.

Note To save the VLAN mappings in the access point after an upgrade or downgrade, you should restrict the access point join is restricted to the controller for which it is primed. No other discoverable controller with a different configuration should be available by other means. Similarly, at the time the access point joins, if it moves across controllers that have different VLAN mappings, the VLAN mappings at the access point might get mismatched.

Commands Related to Configuring the Access Point for FlexConnect

Use these commands on the FlexConnect access point to get status information:

- **show capwap reap status**—Shows the status of the FlexConnect access point (connected or standalone).
- **show capwap reap association**—Shows the list of clients associated to this access point and their SSIDs.

Use these commands on the FlexConnect access point to get debug information:

- **debug capwap reap**—Shows general FlexConnect activities.
- **debug capwap reap mgmt**—Shows client authentication and association messages.
- **debug capwap reap load**—Shows payload activities, which is useful when the FlexConnect access point boots up in standalone mode.
- **debug dot11 mgmt interface**—Shows 802.11 management interface events.
- **debug dot11 mgmt msg**—Shows 802.11 management messages.
- **debug dot11 mgmt ssid**—Shows SSID management events.
- **debug dot11 mgmt state-machine**—Shows the 802.11 state machine.
- **debug dot11 mgmt station**—Shows client events.

Configuring an Access Point for Local Authentication on a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID of the WLAN. The WLANs > Edit page appears.

Step 3 Click the **Advanced** tab to open the WLANs > Edit (WLAN Name) page.

Step 4 Select the FlexConnect **Local Switching** check box to enable FlexConnect local switching.

Step 5 Select the FlexConnect **Local Auth** check box to enable FlexConnect local authentication.

Caution Do not connect access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

Step 6 Click **Apply** to commit your changes.

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Before you begin, you must have enabled local switching on the WLAN where you want to enable local authentication for an access point. For instructions on how to enable local switching on the WLAN, see the "Configuring the Controller for FlexConnect (CLI)" section on page 16-11.

- **config wlan flexconnect ap-auth** *wlan_id* {**enable** | **disable**}—Configures the access point to enable or disable local authentication on a WLAN.

Caution Do not connect the access points in FlexConnect mode directly to Cisco 2500 Series Controllers.

- **show wlan** *wlan-id* —Displays the configuration for the WLAN. If local authentication is enabled, the following information appears:

```
. . .
. . .
Web Based Authentication..................... Disabled
   Web-Passthrough........................... Disabled
   Conditional Web Redirect.................. Disabled
   Splash-Page Web Redirect.................. Disabled
   Auto Anchor............................... Disabled
   FlexConnect Local Switching.................. Enabled
   FlexConnect Local Authentication............. Enabled
   FlexConnect Learn IP Address................. Enabled
   Client MFP................................ Optional
   Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping................................. Disabled
Roamed Call Re-Anchor Policy.................. Disabled
. . .
. . .
```

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the "Configuring the Controller for FlexConnect" section on page 16-8.

In the example scenarios (see Table 16-1), there are three profiles on the client:

1. To connect to the “employee” WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. After the client becomes authenticated, the client gets an IP address from the management VLAN of the controller.
2. To connect to the “local-employee” WLAN, create a client profile that uses WPA/WPA2 authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the local switch.
3. To connect to the “guest-central” WLAN, create a client profile that uses open authentication. After the client becomes authenticated, the client gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user can type any http address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters the username and password.

To determine if a client’s data traffic is being locally or centrally switched, choose **Monitor > Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the Data Switching parameter under AP Properties.

Configuring FlexConnect ACLs

This section contains the following topics:

Information About Access Control Lists

An access control list (ACL) is a set of rules that are used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs enable access control of network traffic. After ACLs are configured on the controller and subsequently pushed to the FlexConnect access point, you can apply them to the access point’s VLAN interface. ACLs enable you to control data traffic to and from wireless clients. You can configure ACLs on the FlexConnect access points to enable effective usage and access control of locally switched data traffic on an access point.

Guidelines and Limitations

- FlexConnect ACLs can only be applied to FlexConnect access points. The configurations applied are per AP, per VLAN.
- The FlexConnect ACLs can be applied to VLAN interfaces on access points in both the Ingress and Egress mode.
- Existing interfaces on an access point can be mapped to ACLs. The interfaces can be created configuring a WLAN-VLAN mapping on the FlexConnect access point.
- The FlexConnect ACLs can be applied to an access point’s VLAN only if VLAN support is enabled on the FlexConnect access point.
- Non-FlexConnect ACLs configured on the controller cannot be applied to a FlexConnect AP.

- FlexConnect ACLs do not support direction per rule. Unlike normal ACLs, Flexconnect ACLs cannot be configured with a direction. An ACL as a whole needs to be applied to an interface as Ingress or Egress.
- You can define up to 512 FlexConnect ACLs, each with up to 64 rules (or filters). Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet.
- ACLs in your network might need to be modified if CAPWAP uses different ports than LWAPP.
- All ACLs have an implicit “deny all rule” as the last rule. If a packet does not match any of the rules, it is dropped by the FlexConnect access point.
- FlexConnect ACLs cannot be combined with Local mode ACLs on the same WLAN. If ACLs are needed for both FlexConnect and Local mode APs, you can apply two different WLANs to support the use of ACLs in both operating modes (one WLAN for FlexConnect APs and the other WLAN for Local mode APs).
- ACLs mapping on the VLANs which are created on the AP using WLAN-VLAN mapping, must be done on a per AP basis only. VLANs can be created on a FlexConnect group for AAA override. These VLANs will not have any mapping for a WLAN. ACLs for VLANs created on the FlexConnect group, must be mapped on the FlexConnect group only. In case the same VLAN is present on the AP as well as the Flexconnect group, AP VLAN will take priority. This means if no ACL is mapped on the AP, the VLAN will not have any ACL, even if the ACL is mapped to the VLAN on the FlexConnect group.

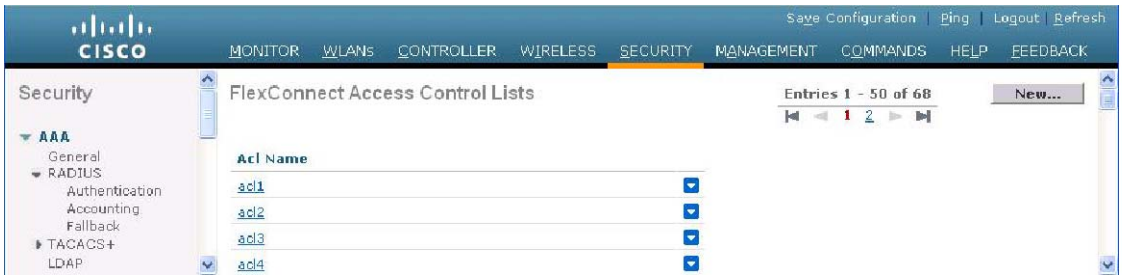
Configuring FlexConnect ACLs

This section contains the following topics:

Configuring FlexConnect ACLs (GUI)

Step 1 Choose **Security > Access Control Lists > FlexConnect ACLs**.

Figure 16-4 FlexConnect ACLs Page



This page lists all FlexConnect ACLs created and configured on the controller. To remove an ACL, hover your mouse over the blue drop-down arrow and choose **Remove**.

Step 2 Add a new ACL by clicking **New**.

The **Access Control Lists > New** page appears.

Step 3 In the Access Control List Name text box, enter a name for the new ACL.

You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

When the Access Control Lists page reappears, click the name of the new ACL.

Step 5 When the Access Control Lists > Edit page appears, click **Add New Rule**.

The Access Control Lists > Rules > New page appears.

Step 6 Configure a rule for this ACL as follows:

a. The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

b. From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

- **Any**—Any source (this is the default value).
- **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the text boxes.

c. From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any**—Any destination (this is the default value).
- **IP Address**—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.

d. From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can choose are as follows:

- **Any**—Any protocol (this is the default value)
- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol

Note If you choose **Other**, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The access point can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

If you chose TCP or UDP, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

e. From the DSCP drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.
   - **Any**—Any DSCP (this is the default value)
   - **Specific**—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

f. From the Action drop-down list, choose **Deny** to cause this ACL to block packets or **Permit** to cause this ACL to allow packets. The default value is Deny.

g. Click **Apply** to commit your changes. The Access Control Lists > Edit page reappears, showing the rules for this ACL.

h. Repeat this procedure to add any additional rules for this ACL.

Step 7 Click **Save Configuration** to save your changes.

Configuring FlexConnect ACLs (CLI)

- **config flexconnect acl create** *name*—Creates an ACL on a FlexConnect access point. The name must be an IPv4 ACL name of up to 32 characters.
- **config flexconnect acl delete** *name*—Deletes a FlexConnect ACL.
- **config flexconnect acl rule action acl-name** *rule-index* **{permit |deny}—**Permits or denies an ACL.
- **config flexconnect acl rule add** *acl-name rule-index*—Adds an ACL rule.
- **config flexconnect acl rule change index** *acl-name old-index new-index*—Changes the index value for an ACL rule.
- **config flexconnect acl rule delete** *name*—Deletes an ACL rule.
- **config flexconnect acl rule dscp** *acl-name rule-index* **{0-63 | any }**—Specifies the differentiated services code point (DSCP) value of this rule index. DSCP is an IP header that can be used to define the quality of service across the Internet. Enter a value between 0 and 63 or ‘any’. The default is ‘any.’
- **config flexconnect acl rule protocol acl-name** *rule-index* **{0-255 | any}**—Assigns the rule index to an ACL rule. Specify a value between 0 and 255 or any. The default is any.
- **config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask*—Configures a rule's destination IP address, netmask and port range.
- **config flexconnect acl rule destination port range** *acl-name rule-index start-port end-port*—Configures a rule’s destination port range.

- **config flexconnect acl rule source address** *acl-name rule-index ipv4-addr subnet-mask*—Configures a rule's source IP address and netmask.
- **config flexconnect acl rule source port range** *acl-name rule-index start-port end-port*—Configures a rule's source port range.
- **config flexconnect acl apply** *acl-name*—Applies the ACL to the FlexConnect access point.
- **config flexconnectacl rule swap** *acl-name index-1 index-2*—Swaps the index values of two rules.
- **config ap flexconnect vlan add** *acl vlan-id ingress-aclname egress-acl-name ap-name*—Maps an ACL to an existing VLAN configured through WLAN-VLAN mapping.

Viewing and Debugging FlexConnect ACLs (CLI)

- **show flexconnect acl summary**—Displays a summary of the access control lists.
- **show flexconnect acl detailed acl-name**—Displays the detailed ACL information for the access control list.
- **debug flexconnect acl {enable | disable}**—Enables or disables FlexConnect ACL. Use this command to troubleshoot.
- **debug capwap reap**—Displays the debug messages for the FlexConnect ACLs on a FlexConnect access point.

Configuring FlexConnect Groups

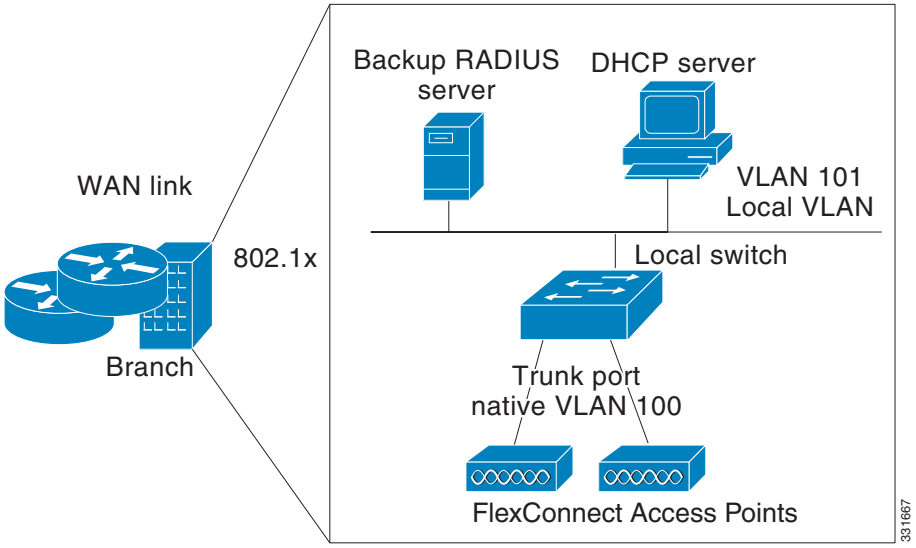
This section contains the following topics:

Information About FlexConnect Groups

To organize and manage your FlexConnect access points, you can create FlexConnect Groups and assign specific access points to them.

All of the FlexConnect access points in a group share the same backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect rather than having to configure the same server on each access point. Figure 16-5 shows a typical FlexConnect deployment with a backup RADIUS server in the branch office.

Figure 16-5 FlexConnect Group Deployment



FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. You can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers can be used when the FlexConnect access point is in of these two modes: standalone or connected.

FlexConnect Groups and CCKM

FlexConnect Groups are required for CCKM fast roaming to work with FlexConnect access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect that includes a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

Note CCKM fast roaming among FlexConnect and non-FlexConnect access points is not supported. See the "Configuring WPA1 +WPA2" section on page 8-26 for information on configuring CCKM.

FlexConnect Groups and Opportunistic Key Caching

Starting in the 7.0.116.0 release, FlexConnect groups enable Opportunistic Key Caching (OKC) to enable fast roaming of clients. OKC facilitates fast roaming by using PMK caching in access points that are in the same FlexConnect group.

This feature prevents the need to perform a full authentication as the client roams from one access point to another. Whenever a client roams from one FlexConnect access point to another, the FlexConnect group access point calculates the PMKID using the cached PMK.

To see the PMK cache entries at the FlexConnect access point, use the **show capwap reap pmk** command. This feature is supported on Cisco FlexConnect access points.

Note The FlexConnect access point must be in connected mode when the PMK is derived during WPA2/802.1x authentication.

When using FlexConenct groups for OKC or CCKM, the PMK-cache is shared only across the access points that are part of the same FlexConnect group and are associated to the same controller. If the access points are in the same FlexConnect group but are associated to different controllers that are part of the same mobility group, the PMK cache is not updated and CCKM roaming will fail.

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database or adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

Note This feature can be used with the FlexConnect backup RADIUS server feature. If a FlexConnect is configured with both a backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect access point itself (if the primary and secondary are not reachable).

The number of FlexConnect groups and access point support depends on the platform that you are using. You can configure the following:

- Up to 100 FlexConnect groups for a Cisco 5500 Series Controller
- Up to 1000 FlexConnect groups for a Cisco Flex 7500 Series Controller. The Cisco Flex 7500 Series Controller can accommodate up to 50 access points per FlexConnect group.
- Up to 20 FlexConnect groups with up to 25 access points per group for the remaining platforms.

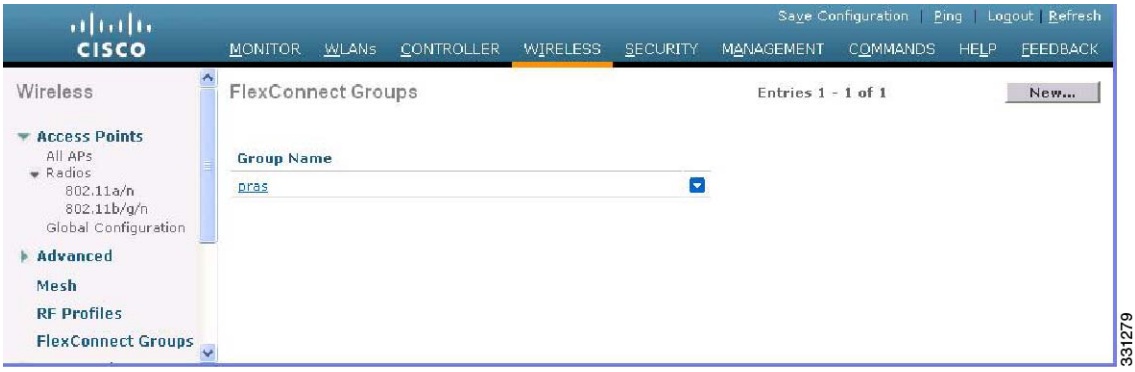
Configuring FlexConnect Groups

This section contains the following topics:

Configuring FlexConnect Groups (GUI)

Step 1 Choose **Wireless** > FlexConnect **Groups** to open the FlexConnect Groups page.

Figure 16-6 FlexConnect Groups Page



This page lists any FlexConnect groups that have already been created.

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

Step 2 Click **New** to create a new FlexConnect Group.

Step 3 On the FlexConnect Groups > New page, enter the name of the new group in the Group Name text box. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply** to commit your changes. The new group appears on the FlexConnect Groups page.

Step 5 To edit the properties of a group, click the name of the desired group. The FlexConnect Groups > Edit page appears.

Step 6 If you want to configure a primary RADIUS server for this group (for example, the access points are using 802.1X authentication), choose the desired server from the Primary RADIUS Server drop-down list. Otherwise, leave the text box set to the default value of None.

Step 7 If you want to configure a secondary RADIUS server for this group, choose the server from the Secondary RADIUS Server drop-down list. Otherwise, leave the field set to the default value of None.

Step 8 To add an access point to the group, click **Add AP**. Additional fields appear on the page under Add AP.

Step 9 Perform one of the following tasks:

- To choose an access point that is connected to this controller, select the **Select APs from Current Controller** check box and choose the name of the access point from the AP Name drop-down list.

  Note If you choose an access point on this controller, the MAC address of the access point is automatically entered in the Ethernet MAC text box to prevent any mismatches from occurring.

- To choose an access point that is connected to a different controller, leave the **Select APs from Current Controller** check box unselected and enter its MAC address in the Ethernet MAC text box.

Note If the FlexConnect access points within a group are connected to different controllers, all of the controllers must belong to the same mobility group.

Step 10 Click **Add** to add the access point to this FlexConnect group. The access point's MAC address, name, and status appear at the bottom of the page.

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

Step 11 Click **Apply** to commit your changes.

Step 12 Repeat Step 9 through Step 11 if you want to add more access points to this FlexConnect Group.

Step 13 Enable local authentication for a FlexConnect Group as follows:

a. Ensure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to None.

b. Select the **Enable AP Local Authentication** check box to enable local authentication for this FlexConnect Group. The default value is unselected.

c. Click **Apply** to commit your changes.

d. Click the **Local Authentication** tab to open the FlexConnect > Edit (Local Authentication > Local Users) page.

e. To add clients that you want to be able to authenticate using LEAP or EAP-FAST, perform one of the following:

- Upload a comma-separated values (CSV) file by selecting the **Upload CSV File** check box, clicking the **Browse** button to browse to an CSV file that contains usernames and passwords (each line of the file needs to be in the following format: username, password), and clicking **Add** to upload the CSV file. The clients' names appear on the left side of the page under the "User Name" heading.
- Add clients individually by entering the client's username in the User Name text box and a password for the client in the Password and Confirm Password text boxes, and clicking **Add** to add this client to the list of supported local users. The client name appears on the left side of the page under the "User Name" heading.

Note You can add up to 100 clients.

f. Click **Apply** to commit your changes.

g. Click the **Protocols** tab to open the FlexConnect > Edit (Local Authentication > Protocols) page.

h. To allow a FlexConnect access point to authenticate clients using LEAP, select the **Enable LEAP Authentication** check box and then go to Step n.

i. To allow a FlexConnect access point to authenticate clients using EAP-FAST, select the **Enable EAP-FAST Authentication** check box and then go to the next step. The default value is unselected.

j. Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the server key used to encrypt and decrypt PACs in the Server Key and Confirm Server Key text boxes. The key must be 32 hexadecimal characters.

- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Enable Auto Key Generation** check box.

k. In the Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

l. In the Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

m. To specify a PAC timeout value, select the **PAC Timeout** check box and enter the number of seconds for the PAC to remain viable in the text box. The default value is unselected, and the valid range is 2 to 4095 seconds when enabled.

n. Click **Apply** to commit your changes.

Step 14 Click **Save Configuration** to save your changes.

Step 15 Repeat this procedure if you want to add more FlexConnects.

Note To see if an individual access point belongs to a FlexConnect Group, you can choose **Wireless > Access Points > All APs >** the name of the desired access point in the FlexConnect tab. If the access point belongs to a FlexConnect, the name of the group appears in the FlexConnect Name text box.

Configuring FlexConnect Groups (CLI)

Step 1 Add or delete a FlexConnect Group by entering this command:

config flexconnect *group_name* {**add** | **delete**}

Step 2 Configure a primary or secondary RADIUS server for the FlexConnect Group by entering this command:

config flexconnect *group_name* **radius server** {**add** | **delete**} {**primary** | **secondary**} *server_index*

Step 3 Add an access point to the FlexConnect Group by entering this command:

config flexconnect *group_name* **ap** {**add** | **delete**} *ap_mac*

Step 4 Configure local authentication for a FlexConnect group as follows:

a. Make sure that a primary and secondary RADIUS server are not configured for the FlexConnect Group.

b. To enable or disable local authentication for this FlexConnect group, enter this command:

config flexconnect *group_name* **radius ap** {**enable** | **disable**}

c. To enter the username and password of a client that you want to be able to authenticate using LEAP or EAP-FAST, enter this command:

config flexconnect *group_name* **radius ap user add** *username* **password** *password*

Note You can add up to 100 clients.

d. To allow a FlexConnect access point to authenticate clients using LEAP or to disable this behavior, enter this command:

config flexconnect *group_name* **radius ap leap** {**enable** | **disable**}

e. To allow a FlexConnect access point to authenticate clients using EAP-FAST or to disable this behavior, enter this command:

config flexconnect *group_name* **radius ap eap-fast** {**enable** | **disable**}

f. Enter one of the following commands, depending on how you want PACs to be provisioned:

- **config flexconnect** *group_name* **radius ap server-key** *key*—Specifies the server key used to encrypt and decrypt PACs. The key must be 32 hexadecimal characters.
- **config flexconnect** *group_name* **radius ap server-key auto**—Allows PACs to be sent automatically to clients that do not have one during PAC provisioning.

g. To specify the authority identifier of the EAP-FAST server, enter this command:

config flexconnect *group_name* **radius ap authority id** *id*

where *id* is 32 hexadecimal characters.

h. To specify the authority identifier of the EAP-FAST server in text format, enter this command:

config flexconnect *group_name* **radius ap authority info** *info*

where *info is up to 32 hexadecimal characters.*

i. To specify the number of seconds for the PAC to remain viable, enter this command:

config flexconnect *group_name* **radius ap pac-timeout** *timeout*

where *timeout is a value between 2 and* 4095 seconds (inclusive) or 0. A value of 0, which the default value, disables the PAC timeout.

Step 5 Save your changes by entering this command:

save config

Step 6 See the current list of FlexConnect Groups by entering this command:

show flexconnect summary

Information similar to the following appears:

```
flexconnect Summary: Count 2

Group Name     # Aps
Group 1        1
Group 2        1
```

Step 7 See the details for a specific FlexConnect Groups by entering this command:

show flexconnect group detail *group_name*

Information similar to the following appears:

```
Number of Ap's in Group: 3

00:1d:45:12:f2:24    AP1240.EW3.f224  Joined
00:1d:45:12:f7:12    AP1240.10.f712     Joined
00:1d:a1:ed:9f:84    AP1131.23.9f84     Joined

Group Radius Servers Settings:
 Primary Server Index.......................... Disabled
 Secondary Server Index........................ Disabled

Group Radius AP Settings:
AP RADIUS server............ Enabled
EAP-FAST Auth............... Enabled
LEAP Auth................... Enabled
Server Key Auto Generated... No
```

```
Server Key.................     <hidden>
Authority ID................ 436973636f00000000000000000000000
Authority Info.............. Cisco A_ID
PAC Timeout................. 0
Number of User's in Group: 20

                  1cisco                    2cisco
                  3cisco                    4cisco
                   cisco                     test1
                  test10                    test11
                  test12                    test13
                  test14                    test15
                   test2                     test3
                   test4                     test5
                   test6                     test7
                 test8                   test9
```

Configuring VLAN-ACL Mapping on FlexConnect Groups (GUI)

Step 1 Choose **Wireless > FlexConnect Groups**.

The FlexConnect Groups page appears. This page lists the access points associated with the controller.

Step 2 Click the Group Name link of the FlexConnect Group for which you want to configure VLAN-ACL mapping.

Step 3 Click the **VLAN-ACL** Mapping tab.

The VLAN-ACL Mapping page for that FlexConnect group is displayed.

Step 4 Enter the Native VLAN ID in the VLAN ID text box.

Step 5 From the Ingress ACL drop-down list, choose the Ingress ACL.

Step 6 From the Egress ACL drop-down list, choose the Egress ACL.

Step 7 Click **Add** to add this mapping to the FlexConnect Group.

The VLAN ID is mapped with the required ACLs. To remove the mapping, hover your mouse over the blue drop-down arrow and choose **Remove**.

Configuring VLAN-ACL Mapping on FlexConnect Groups (CLI)

- **config flexconnect group** *group-name* **vlan add** *vlan-id* acl *ingress-acl egress-acl*—Adds a VLAN to a FlexConnect group and maps the ingress and egress ACLs.

Viewing VLAN-ACL Mappings (CLI)

- **show flexconnect group detail** *group-name*—Displays the FlexConnect group details.
- **show ap config general** *ap-name*—Displays the VLAN-ACL mappings on the access point. An output similar to the following is displayed:

```
.. . .
. . . . .
FlexConnect Vlan mode ..................... Enabled
```

```
        Native ID :..................................... 45
        WLAN 1 :........................................ 45
FlexConnect VLAN ACL Mappings
Vlan :.......................................... 45
        Ingress ACL :................................... None
        Egress ACL :.................................... None
VLAN with least priority :...................... 75
FlexConnect Group.............................. fc-grp-1
Group VLAN ACL Mappings
Vlan :.......................................... 61
        Ingress ACL :................................... fc-grp-65
        Egress ACL :.................................... fc-grp-81
Vlan :.......................................... 62
        Ingress ACL :................................... fc-grp-66
        Egress ACL :.................................... fc-grp-82
Vlan :.......................................... 63
        Ingress ACL :................................... fc-grp-67
        Egress ACL :.................................... fc-grp-83
Vlan :.......................................... 64
        Ingress ACL :................................... fc-grp-68
        Egress ACL :.................................... fc-grp-84
Vlan :.......................................... 65
        Ingress ACL :................................... fc-grp-69
        Egress ACL :.................................... fc-grp-85
. . .
. . .
```

- The **VLAN with least priority—**Specifies the least priority VLANs from the list of VLANs added to the access point using the WLAN-VLAN mapping. If the a VLAN is added and if it exceeds the maximum allowed VLANs (16) on the AP, the VLAN specified in this section is replaced.
- **FlexConnect VLAN ACL Mappings**—Refers to the configuration of VLANs done using WLAN-VLAN mappings on a per-AP basis using the **config ap flexconnect vlan add** comm and.
- **Group VLAN ACL Mappings**—Refers to the configuration of VLAN and the corrsponding Ingress and Egress ACLs on a FlexConnect group that is pushed to the access point using the **config flexconnect group** *group-name* **vlan add** command**.**

Configuring AAA Overrides for FlexConnect

This section contains the following topics:

Information About AAA Overrides

The Allow AAA Override option of a WLAN enables you to configure the WLAN for authentication. It enables you to apply VLAN tagging to individual clients based on the returned RADIUS attribute from the AAA server.

AAA overrides for FlexConnect access points introduce a dynamic VLAN assignment for locally switched clients. AAA overrides for FlexConnect also supports fast roaming (OKC/CCKM) of overridden clients.

Guidelines and Limitations

- VLAN overrides for FlexConnect is applicable for both centrally and locally authenticated clients.
- Before configuring an AAA override, the VLAN must be created on the access points. These VLANs can be created on the access points by using the existing WLAN-VLAN mappings.
- VLANs can be configured on FlexConnect groups. VLANs are pushed to the access points belonging to the FlexConnect group.
- At any given point, an AP has a maximum of 16 VLANs. The VLANs are selected based on the WLAN-VLAN mapping in the AP . The remaining VLANs will be pushed from the Flexconnect group in the order that they are configured/shown in the Flexconnect group. If the VLAN slots are full, an error message is logged.
- If the VLAN on the AP is configured using the WLAN-VLAN, the AP configuration of the ACL is applied.
- If the VLAN is configured using the FlexConnect group, the ACL configured on the FlexConnect group is applied.
- If the same VLAN is configured on the FlexConnect group and also at the AP, the AP configuration with its ACL takes precedence.
- If there is no slot for a new VLAN from the WLAN-VLAN mapping, the latest FlexConnect group VLAN is replaced.
- If the VLAN that was returned from the AAA is not present on the AP, the client falls back to the default VLAN configured for the WLAN.
- AAA for locally switched clients only supports VLAN overrides.
- AAA Override for FlexConnect is supported through IETF parameters in the ACS. The following parameters must be configured with the specified values as defined below for a user:
  - [064] Tunnel-Type : Tag 1 value VLAN
  - [065] Tunnel-Medium Type : Tag1 value 802
  - [081] Tunnel-Private-Group-ID : Tag1 value : *Overridden VLAN ID.*
- Dynamic VLAN assignment is not supported for web authentication from a controller with ACS.

Note To know more about how to configure IETF parameters, refer to the documentation of ACS server you are using.

Configuring AAA Override for FlexConnect on an Access Point (GUI)

Step 1 Choose **Wireless > All APs**.

The All APs appears. This page lists the access points associated with the controller.

Step 2 Click the **AP name** link of the access point for which you want to configure VLAN Override.

Step 3 Click the **FlexConnect** tab.

Step 4 Enter the Native VLAN ID.

Step 5 Click the **VLAN Mappings** button to configure the AP VLANs mappings. This page displays the following parameters:

- AP Name—The access point name.
- Base Radio MAC—The base radio of the AP.
- WLAN-SSID-VLAN ID Mappings—For each WLAN configured on the controller, the corresponding SSID and VLAN IDs are listed. Change the WLAN-VLAN ID mappings by editing the VLAN ID column for a WLAN.
- Centrally Switched WLANs—If centrally switched WLANs are configured, the WLAN–VLAN mapping is listed.
- AP Level VLAN ACL Mapping—Change the ingress ACL and egress ACL mappings by choosing the mappings from the drop-down list for each ACL type. The following parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The ingress ACL that corresponds to the VLAN.
  - Egress ACL—The egress ACL that corresponds to the VLAN.
- Group Level VLAN ACL Mappings—The following group level VLAN ACL mapping parameters are available:
  - VLAN ID—The VLAN ID.
  - Ingress ACL—The ingress ACL for this VLAN.
  - Egress ACL—The egress ACL for this VLAN.

Step 6 Click **Apply**.

Configuring VLAN Overrides for FlexConnect on an Access Point (CLI)

Step 1 Add a VLAN to a FlexConnect group and map the ingress and egress ACLs:

config flexconnect group *group-name* **vlan add** *vlan-id acl ingress-acl egress-acl*

Note Use the **none** keyword in place of ‘ingress-acl’ or ‘egress-acl’ If you do not want to set a value to the ACL You can also use the **none** keyword to clear the ACL.

Step 2 Enable AAA override on the WLAN using the following command:

config wlan aaa-override enable *wlan_id*

Configuring Efficient AP Image Upgrades for FlexConnect Access Points

This section contains the following topics:

- Configuring Efficient AP Image Upgrades (CLI), page 16-32

Information About Efficient AP Image Upgrades

Normally, when upgrading the image of an AP, you can use the preimage download feature to reduce the amount of time that the AP is unavailable to serve clients. However, it also increases the downtime because the access point cannot serve clients during an upgrade. The preimage download feature can be used to reduce this downtime. However, in the case of a branch office setup, the upgrade images are still downloaded to each access point over the WAN link, which has a higher latency.

A more efficient way is to use the Efficient AP Image Upgrade feature. When the Efficient Image Upgrade feature is enabled, one access point of each model in the local network first downloads the upgrade image over the WAN link. The process is similar to the master-slave or client-server model. This access point then becomes the master for the remaining access point of the similar model. The remaining access points then download the upgrade image from the master access point using the preimage download feature over the local network, which reduces the WAN latency.

Guidelines and Limitations

- The primary and secondary controllers in the network must have the same set of primary and backup images.
- If you configured a FlexConnect group, all access points in that group must be within the same subnet or must be accessible through NAT.

Configuring Efficient AP Image Upgrades on FlexConnect APs (GUI)

Step 1 Choose **Wireless > FlexConnect Groups**.

The FlexConnect Groups page appears. This page lists the FlexConnect Groups configured on the controller.

Step 2 Click the **Group Name** link on which you want to configure the image upgrade.

Step 3 Click the **Image Upgrade** tab.

Step 4 Select the **FlexConnect AP Upgrade** check box to enable efficient FlexConnect AP Upgrade.

Step 5 If you enabled FlexConnect AP Upgrade in the previous step, you must enable the following parameters:

- **Slave Maximum Retry Count**—The number of attempts that the slave access point must try to connect to the master access point for downloading the upgrade image. If the image download does not occur for the configured retry attempts, the image is upgraded over the WAN.
- **Upgrade Image**—Upgrade image that you can choose. The options are **Primary** and **Backup,** and **Abort**.

Step 6 Click **FlexConnect Upgrade** to upgrade.

Step 7 You can manually assign master access points in the FlexConnect group by selecting the access points from the AP Name drop-down list. Click **Add Master** to add the master access point.

Step 8 Click **Apply**.

Configuring Efficient AP Image Upgrades (CLI)

- **config flexconnect group** *group-name* **predownload {enable | disable}**—Enables or disables the efficient AP upgrade image.
- **config flexconnect group group-name predownload master** *ap-name*—Manually assigns an access point as the master access point.
- **config flexconnect group** *group-name* **predownload slave** *retry-count ap-name*—Sets the access point as a slave access point with a retry count.
- **config flexconnect group group-name predownload start**—Initiates the image download on the access points in the FlexConnect group.
- **config ap image predownload {abort | primary | backup}**—Assigns the image type that must be downloaded for the preimage upgrade.
- **show flexconnect group** *group-name*—Displays the summary of the FlexConnect group configuration.
- **show ap image all**—Displays the details of the images on the access point.