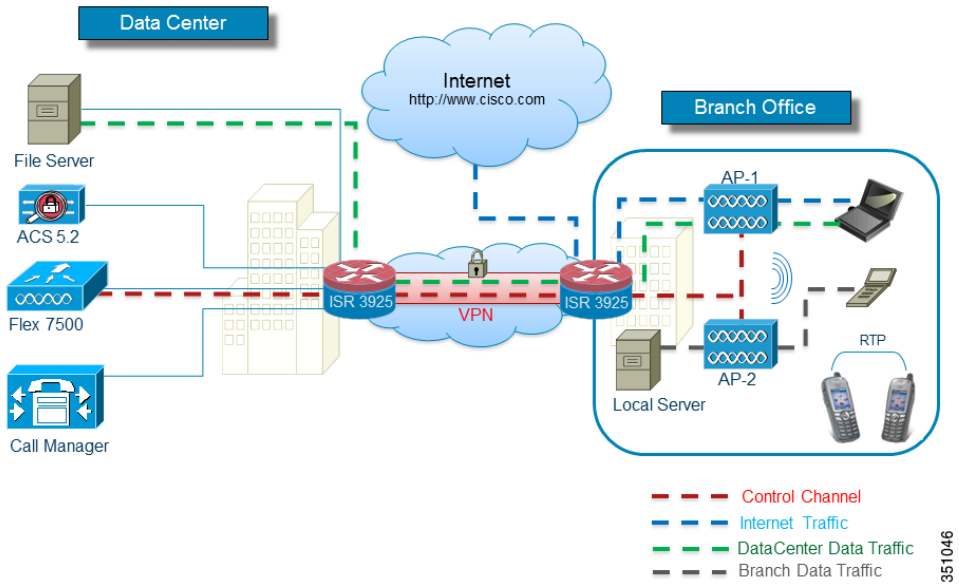
FlexConnect

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 you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without the deployment of a controller in each office. The FlexConnect access points (APs) can switch client data traffic locally and perform client authentication locally. When they are connected to the controller, they can also send traffic back to the controller.

Figure 7-1 FlexConnect Architecture



Note To view the FlexConnect feature matrix, see:
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b3690b.shtml#matrix

Supported Platforms

FlexConnect is only supported on these components:

- Cisco AP-1130, AP-1240, AP-1040, AP-1140, AP-1260, AP-1250, AP-3500, AP-1600, AP-2600, AP-3600, AP-3700, AP-1700, AP-2700, AP 700, AP-1520, AP-1530, AP-1550, AP-1570 access points
- Cisco 5520, 8540, Flex 7500, Cisco 8500, 4400, 5500, and 2500 series controllers
- Cisco WiSM-2
- Cisco virtual controller (vWLC)

FlexConnect Terminology

For clarity, this section provides a summary of the FlexConnect terminology and definitions used throughout this chapter.

Switching Modes

FlexConnect APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis.

Local Switched

Locally-switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to an adjacent router or switch. If so desired, one or more WLANs can be mapped to the same local 802.1Q VLAN.

A branch user, who is associated to a local switched WLAN, has their traffic forwarded by the on-site router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router. All AP control/management-related traffic is sent to the centralized Wireless LAN Controller (WLC) separately via Control and Provisioning of Wireless Access Points protocol (CAPWAP).

Central Switched

Central switched WLANs tunnel both the wireless user traffic and all control traffic via CAPWAP to the centralized WLC where the user traffic is mapped to a dynamic interface/VLAN on the WLC. This is the normal CAPWAP mode of operation.

The traffic of a branch user, who is associated to a central switched WLAN, is tunneled directly to the centralized WLC. If that user needs to communicate with computing resources within the branch (where that client is associated), their data is forwarded as standard IP packets back across the WAN link to the branch location. Depending on the WAN link bandwidth, this might not be desirable behavior.

Operation Modes

There are two modes of operation for the FlexConnect AP.

Connected mode—The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC.

Standalone mode—The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC: for example, when there is a WAN link outage between a branch and its central site.

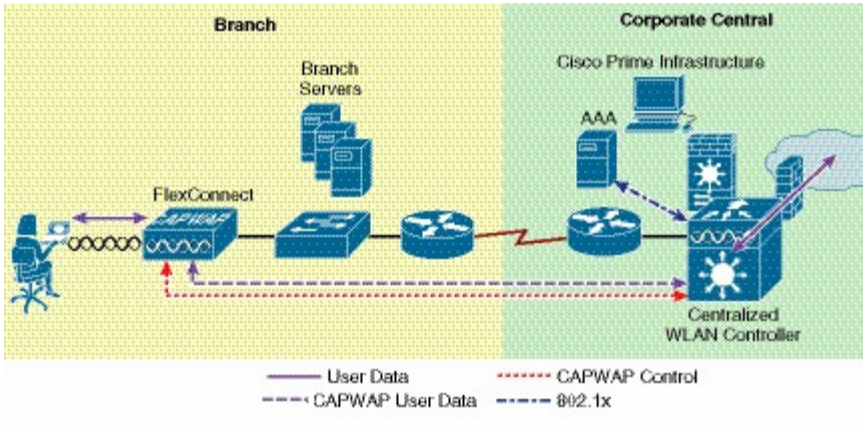
FlexConnect States

A FlexConnect WLAN, depending on its configuration and network connectivity, is classified as being in one of the following defined states.

Authentication-Central/Switch-Central

This state represents a WLAN that uses a centralized authentication method such as 802.1X, VPN, or web. User traffic is sent to the WLC via CAPWAP. This state is supported only when FlexConnect is in connected mode (Figure 7-2); 802.1X is used in the example, but other mechanisms are equally applicable.

Figure 7-2 Authentication-Central/Switch-Central WLAN



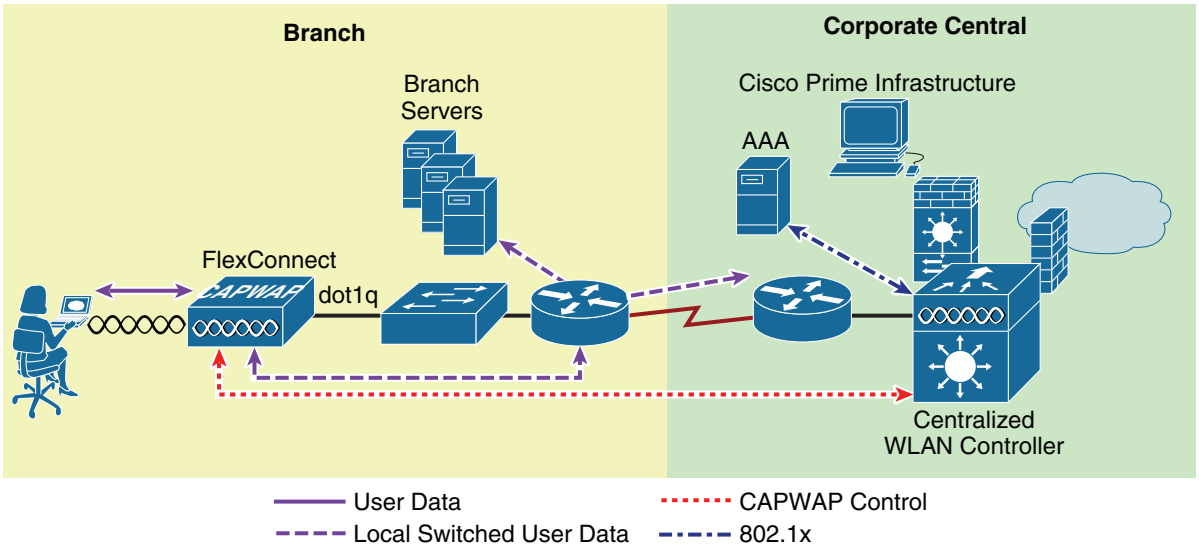
Authentication Down/Switching Down

Central switched WLANs (above) no longer beacon or respond to probe requests when the FlexConnect AP is in standalone mode. Existing clients are disassociated.

Authentication-Central/Switch-Local

This state represents a WLAN that uses centralized authentication, but user traffic is switched locally. This state is supported only when the FlexConnect AP is in connected mode (Figure 7-3); 802.1X is used in the Figure 7-3 example, but other mechanisms are equally applicable.

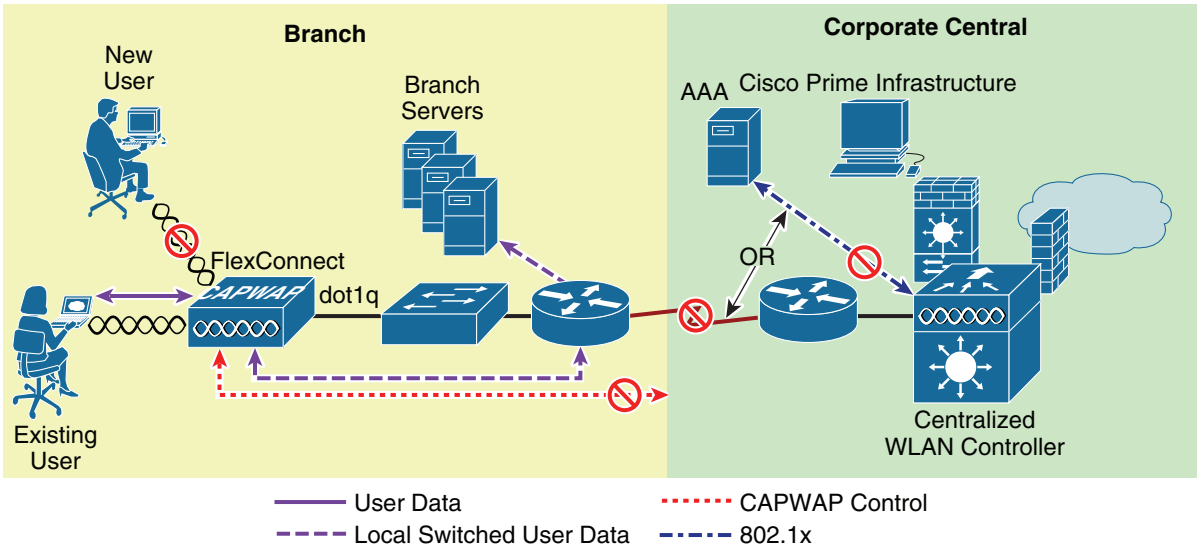
Figure 7-3 Authentication-Central/Switch-Local WLAN



Authentication-Down/Switch-Local

A WLAN that requires central authentication (as explained above) rejects new users. Existing authenticated users continue to be switched locally until session time-out (if configured). The WLAN continues to beacon and respond to probes until there are no more (existing) users associated to the WLAN. This state occurs as a result of the AP going into standalone mode (Figure 7-4).

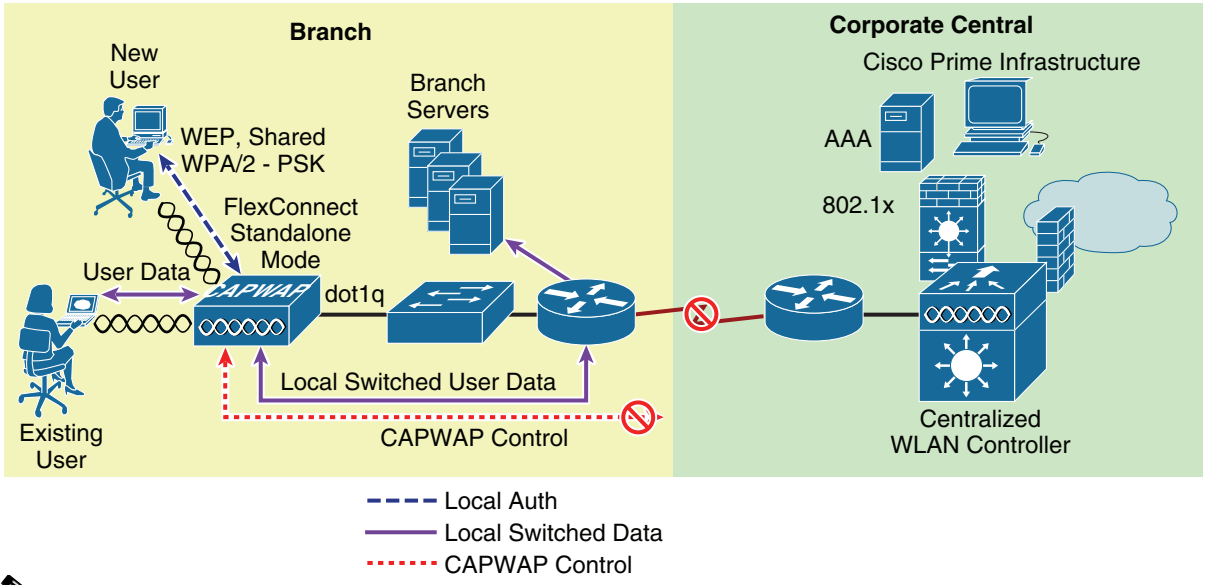
Figure 7-4 Authentication-Down/Local Switch



Authentication-local/switch-local

This state represents a WLAN that uses open, static WEP, shared, or WPA2 PSK security methods. User traffic is switched locally. These are the only security methods supported locally if a FlexConnect goes into standalone mode. The WLAN continues to beacon and respond to probes (Figure 7-5). Existing users remain connected and new user associations are accepted. If the AP is in connected mode, authentication information for these security types is forwarded to the WLC.

Figure 7-5 Authentication-Local/Switch-Local WLAN



Note All 802.11 authentication and association processing occurs regardless of which operational mode the AP is in. When in connected mode, the FlexConnect AP forwards all association/authentication information to the WLC. When in standalone mode, the AP cannot notify the WLC of such events, which is why WLANs that make use of central authentication/switching methods are unavailable.

Applications

The FlexConnect AP offers greater flexibility in how it can be deployed, such as:

- Branch wireless connectivity
- Branch guest access
- Public WLAN hotspot
- Wireless BYOD in Branch sites

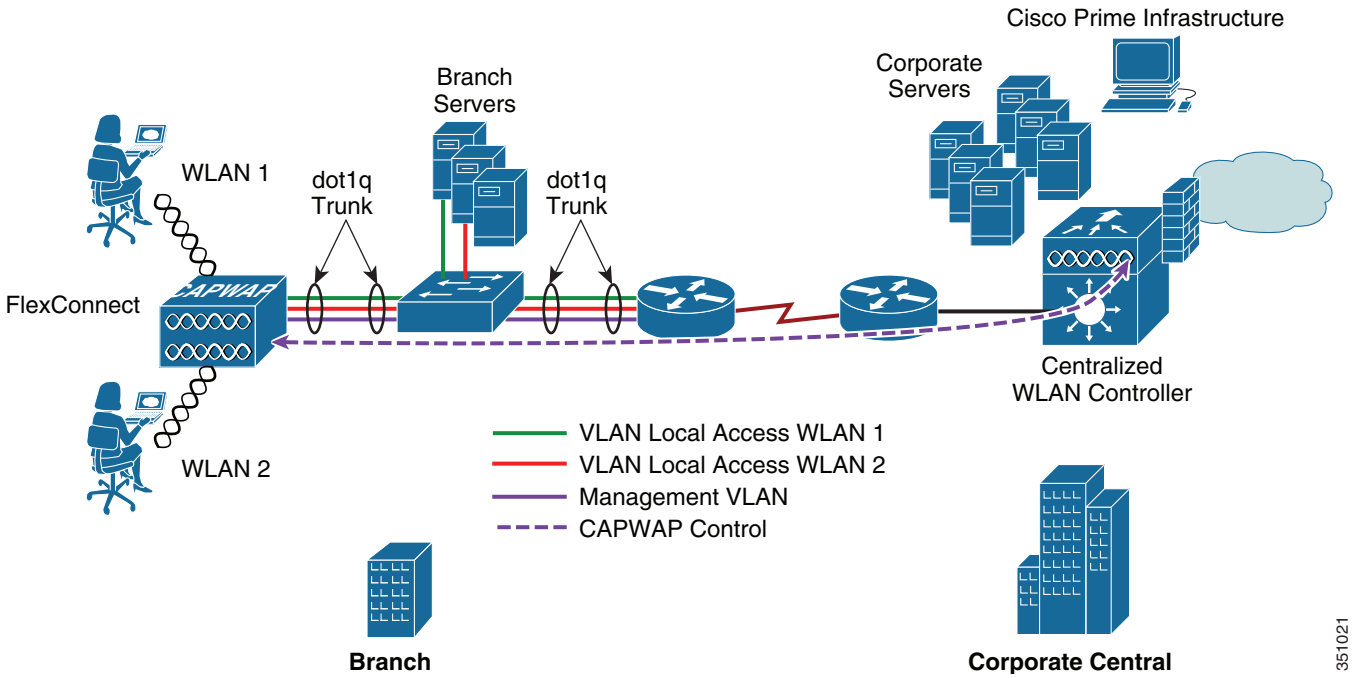
Branch Wireless Connectivity

FlexConnect addresses the wireless connectivity needs in branch locations by permitting wireless user traffic to terminate locally rather than tunneled across the WAN to a central WLC. With FlexConnect, branch locations can more effectively implement segmentation, access control, and QoS policies on a per-WLAN basis, as shown in Figure 7-6.

Branch Guest Access

The centralized WLC itself, as shown in Figure 7-6, can perform web authentication for guest access WLANs. The guest user's traffic is segmented (isolated) from other branch office traffic. For more detailed information on guest access, refer to Chapter 10, "Cisco Unified Wireless Network Guest Access Services."

Figure 7-6 FlexConnect Topology

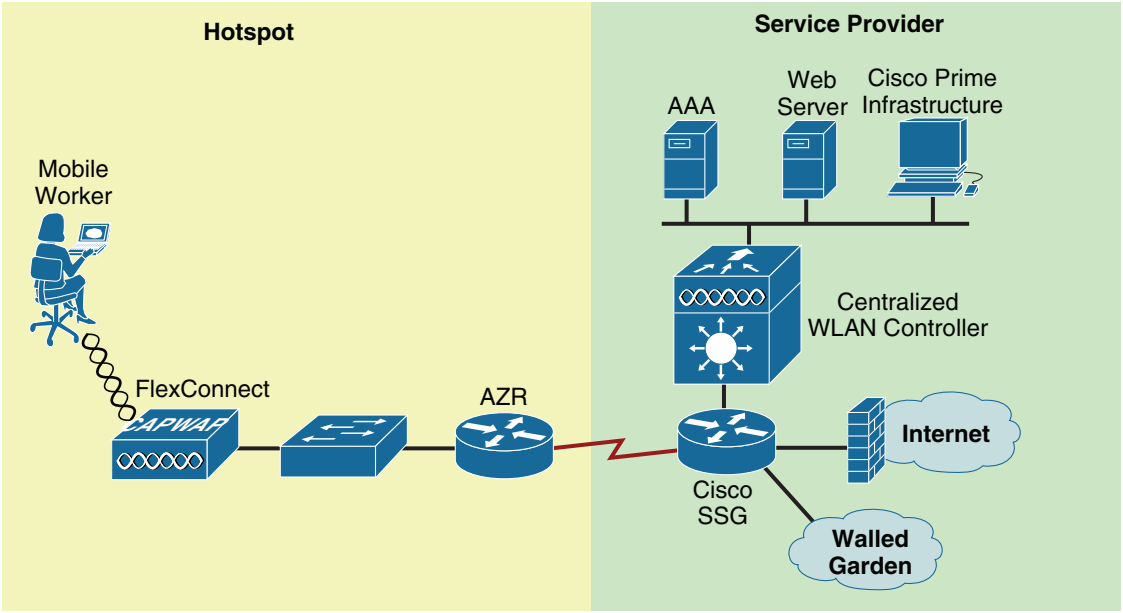


Public WLAN Hotspot

Many public hotspot service providers are beginning to implement multiple SSID/WLANs. One reason for this is because an operator might want to offer an open authentication WLAN for web-based access and another WLAN that uses 802.1x/EAP for more secure public access.

The FlexConnect AP, with its ability to map WLANs to separate VLANs, is an alternative to a standalone AP for small venue hotspot deployments where only one, or possibly two, APs are needed. Figure 7-7 provides an example of hotspot topology using a FlexConnect AP.

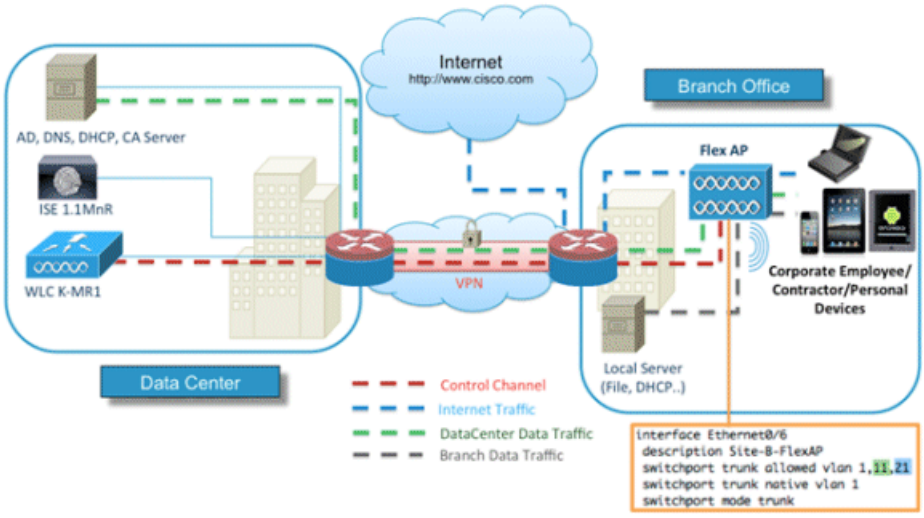
Figure 7-7 Hotspot Access using FlexConnect Local Switching



Wireless BYOD in Branch sites

Release 7.2.110.0 supports these ISE functionalities for FlexConnect APs for local switching and centrally authenticated clients. Also, release 7.2.110.0 integrated with ISE 1.1.1 provides (but is not limited to) these BYOD solution features for wireless:

- Device profiling and posture
- Device registration and supplicant provisioning
- Onboarding of personal devices (provision iOS or Android devices)



Deployment Considerations

The following section covers the various implementation and operational caveats associated with deploying FlexConnect APs.

WAN Link

For the FlexConnect AP to function predictably, keep in mind the following with respect to WAN link characteristics:

- Latency—A given WAN link should not impose latencies greater than 100 ms. The AP sends heartbeat messages to the WLC once every thirty seconds. If a heartbeat response is missed, the AP sends five successive heartbeats (one per second) to determine whether connectivity still exists. If connectivity is lost, the FlexConnect AP switches to standalone mode.

  Similarly, AP and WLC exchange echo CAPWAP packet to check the connectivity. If the echo CAPWAP packet response is missed, the AP sends five successive echo CAPWAP packets (every three seconds) to determine whether the connectivity still exists. If the connectivity is lost, the FlexConnect AP switches to standalone mode. (see Operation Modes, page 7-3 for operation mode definitions). The AP itself is relatively delay tolerant. However, at the client, timers associated with authentication are sensitive to link delay, and thus a constraint of $\leq$ 100 ms is required. Otherwise, the client can time-out waiting to authenticate, which can cause other unpredictable behaviors, such as looping.

- Bandwidth—WAN links should be at least 128 kbps for deployments when up to eight APs are being deployed at a given location. If more than eight APs are deployed, proportionally more bandwidth should be provisioned for the WAN link.

- Path MTU—An MTU no smaller than 500 bytes is required.

Roaming

When a FlexConnect AP is in connected mode, all client probes, association requests, 802.1x authentication requests, and corresponding response messages are exchanged between the AP and the WLC via the CAPWAP control plane. This is true for open, static WEP, and WPA PSK-based WLANs even though CAPWAP connectivity is not required to use these authentication methods when the AP is in standalone mode.

- Dynamic WEP/WPA—A client that roams between FlexConnect APs using one of these key management methods performs full authentication each time it roams. After successful authentication, new keys are passed back to the AP and client. This behavior is no different than a standard centralized WLAN deployment, except that in an FlexConnect topology, there can be link delay variations across the WAN, which can in turn impact total roam time. Depending on the WAN characteristics, RF design, back end authentication network, and authentication protocols being used, roam times may vary.

- WPA2—To improve client roam times, WPA2 introduced key caching capabilities, based on the IEEE 802.11i specification. Cisco created an extension to this specification called Proactive Key Caching (PKC). PKC today is supported only by the Microsoft Zero Config Wireless supplicant and the Funk (Juniper) Odyssey client. Cisco CCKM is also compatible with WPA2.

  Remote branch locations requiring predictable, fast roaming behavior in support of applications such as wireless IP telephony should consider deploying a local WLC (Virtual Controller on UCS blade or 2500 WLC).

- Cisco Centralized Key Management (CCKM)—CCKM is a Cisco-developed protocol in which the WLC caches the security credentials of CCKM-capable clients and forwards those credentials to other APs within a mobility group. When a client roams and associates with another AP, their credentials are forwarded to that AP, which allows the client to re-associate and authenticate in a two-step process. This eliminates the need for full authentication back to the AAA server. CCKM-capable clients undergo full 802.1x authentication each time they roam from one FlexConnect to another.
- FlexConnect Groups are required for CCKM/OKC fast roaming to work with FlexConnect access points. 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/OKC 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/OKC cache for all 100 clients is not practical. If you create a FlexConnect Group comprising 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/OKC cache is distributed among those four access points only when the clients associate to one of them.
- Layer 2 switch CAM table updates—When a client roams from one AP to another on a locally-switched WLAN, FlexConnect does not announce to a Layer 2 switch that the client has changed ports. The switch will not discover that the client has roamed until the client performs an ARP request for its default router. This behavior, while subtle, can have an impact on roaming performance.

Note A client that roams (for a given local switched WLAN) between FlexConnect APs that map the WLAN to a different VLAN/subnet will renew their IP addresses to ensure that they have an appropriate address for the network to which they have roamed.

Radio Resource Management

While in connected mode, all radio resource management (RRM) functionality is fundamentally available. However, because typical FlexConnect deployments comprise a smaller number of APs, RRM functionality might not be operational at a branch location. For example, in order for transmit power control (TPC) to work, there must be a minimum of four FlexConnect APs in proximity to each other. Without TPC, other features such as coverage hole protection will be unavailable.

Location Services

FlexConnect deployments typically consist of only a handful of APs at a given location. Cisco maintains strict guidelines regarding the number and placement of APs to achieve the highest level of location accuracy. As such, although it is possible to obtain location information from FlexConnect deployments, the level of accuracy may vary greatly across remote location deployments.

QoS Considerations

For WLANs that are centrally-switched, the FlexConnect AP handles QoS in the same way as standard APs. Locally-switched WLANs implement QoS differently.

For locally-switched WLANs with Wi-Fi MultiMedia (WMM) traffic, the AP marks the dot1p value within the dot1q VLAN tag for upstream traffic. This happens only for tagged VLANs, not the native VLAN.

For downstream traffic, FlexConnect uses the incoming dot1p tag from the locally-switched Ethernet and uses this to queue and mark the WMM values associated with frames destined to a given user across the RF link.

The WLAN QoS profile is applied both for upstream and downstream packets. For downstream, if an 802.1p value that is higher than the default WLAN value is received, the default WLAN value is used. For upstream, if the client sends a WMM value that is higher than the default WLAN value, the default WLAN value is used. For non-WMM traffic, there is no CoS marking on the client frames from the AP.

For more information see Chapter 5, "Cisco Unified Wireless QoS and AVC."

Note Cisco strongly recommends that appropriate queuing/policing mechanisms be implemented across the WAN to ensure proper handling of traffic based on its DSCP setting. An appropriate priority queue should be reserved for CAPWAP control traffic to ensure that a FlexConnect AP does not inadvertently cycle between connected and standalone modes because of congestion.

FlexConnect Solution

The FlexConnect solution enables you to:

- Centralize control and management traffic.
- Distribute the client data traffic at each Branch Office.
- Ensure traffic flow is going to its final destination in the most efficient manner.

Advantages of Centralizing Access Point Control Traffic

The advantages of centralizing AP control traffic are:

- Single pane of monitoring and troubleshooting
- Ease of management
- Secured and seamless mobile access to Data Center resources
- Reduction in branch footprint
- Increase in operational savings

Advantages of Distributing Client Data Traffic

The advantages of distributing client data traffic are:

- No operational downtime (survivability) against complete WAN link failures or controller unavailability.

- Mobility resiliency within branch during WAN link failures.
- Increase in branch scalability. Supports branch size that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP).

Central Client Data Traffic

The Cisco FlexConnect solution also supports Central Client Data Traffic, but it should be limited to Guest data traffic only. Table 7-1 and Table 7-2 outline the restrictions on WLAN security types only for non-guest clients whose data traffic is also switched centrally at the Data Center.

Table 7-1 Layer 2 Security Support for Centrally-Switched Non-Guest Users

WLAN Layer 2 Security	Type	Results
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	CCKM	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed
CKIP	—	Allowed

Note These authentication restrictions do not apply to clients whose data traffic is distributed at the branch.

Table 7-2 Layer 3 Security Support for Centrally and Locally Switched Users

WLAN Layer 3 Security	Type	Results
Web Authentication	Internal	Allowed
	External	Allowed
	Customized	Allowed
Web Pass-Through	Internal	Allowed
	External	Allowed
	Customized	Allowed
Conditional Web Redirect	External	Allowed
Splash Page Redirect	External	Allowed

Primary Design Requirements

FlexConnect APs are deployed at the Branch site and managed from the Data Center over a WAN link. It is highly recommended that the minimum bandwidth restriction remains 24 kbps per AP with the round trip latency no greater than 300 ms. (see Table 7-3).

The maximum transmission unit (MTU) must be at least 500 bytes.

Table 7-3 Bandwidth Minimums

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	APs per Branch (Max)	Clients per Branch (Max)
Data	64 kbps	300 ms	5	25
Data	640 kbps	300 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Data + Voice	128 kbps	100 ms	5	25
Data + Voice	1.44 Mbps	100 ms	50	1000
Data + Flex AVC	75 Kbps	300 ms	5	25

The primary design requirements are:

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP)
- Central management and troubleshooting
- No operational downtime
- Client-based traffic segmentation
- Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests

FlexConnect Groups

Because all of the FlexConnect APs at each branch site are part of a single FlexConnect Group, FlexConnect Groups ease the organization of each branch site.

Note FlexConnect Groups are not analogous to AP Groups.

The FlexConnect Group is primarily designed to solve the following challenges:

- How can wireless clients perform 802.1X authentication and access Data Center services if the controller fails?
- How can wireless clients perform 802.1X authentication if WAN link between Branch and Data Center fails?
- Is there any impact on branch mobility during WAN failures?

- Does the FlexConnect Solution provide no operational branch downtime?

You can configure the controller to allow a FlexConnect AP, in standalone mode, to perform full 802.1X authentication to a backup RADIUS server.

Note Backup RADIUS accounting is not supported.

To increase the resiliency of the branch, administrators can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers are used only when the FlexConnect AP is not connected to the controller.

Configuring FlexConnect Groups

Complete the following procedure to configure FlexConnect groups to support Local Authentication using Local Extensible Authentication Protocol (LEAP), when FlexConnect is either in connected or standalone mode.

Step 1 Click **New** under **Wireless > FlexConnect Groups**.

Step 2 Assign **Group Name** as Store 1.

Step 3 Click **Apply** when the Group Name is set.

Step 4 Click the newly created Group Name Store 1.

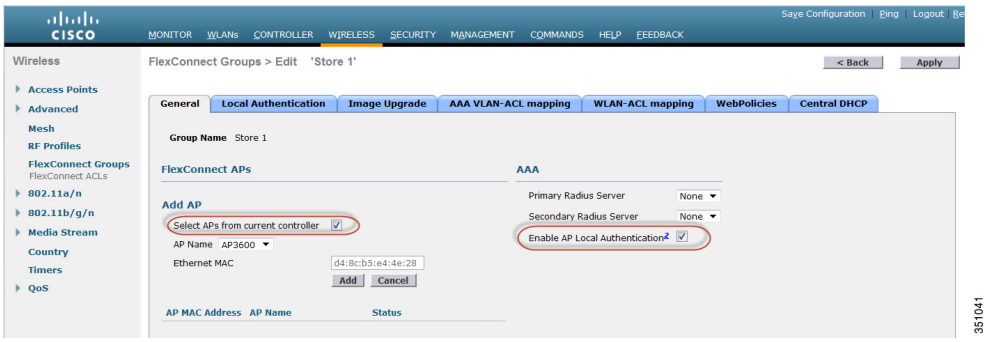
Step 5 Click **Add AP**.

Step 6 Check the **Enable AP Local Authentication** check box to enable Local Authentication when the AP is in standalone mode.

Step 7 Check the **Select APs from current controller** check box to enable the **AP Name** drop-down menu.

Step 8 Choose the AP from the **AP Name** drop-down menu that needs to be part of this FlexConnect Group.

Step 9 Click **Add**.



Step 10 Repeat Step 7 and Step 8 to add all of the APs to this FlexConnect Group Store 1.

Note Maintaining 1:1 ratio between the AP-Group and FlexConnect group simplifies network management.

Step 11 Navigate to **Local Authentication > Protocols** tabs and then check the **Enable LEAP Authentication** check box.

Step 12 Click **Apply**.

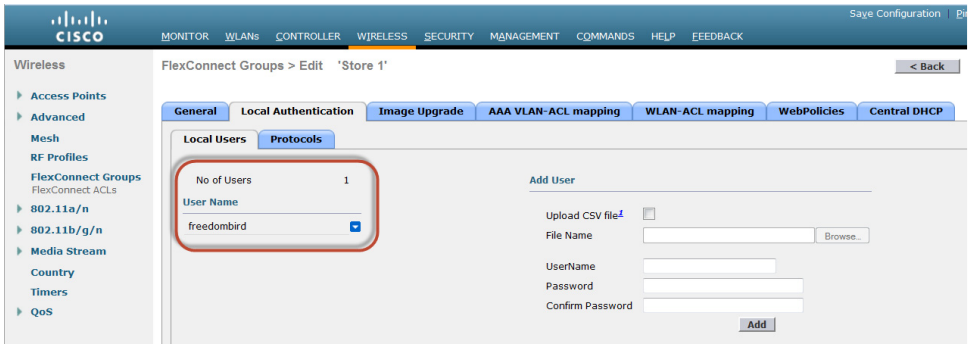
Note If you have a backup controller, make sure the FlexConnect groups are identical and AP MAC address entries are included per FlexConnect group.

Step 13 Navigate to **Local Authentication > Local Users** tabs.

Step 14 Set the **UserName**, **Password** and **Confirm Password** fields, and then click **Add** to create user entry in the LEAP server residing on the AP.

Step 15 Repeat Step 13 until your local username list is exhausted. You cannot configure or add more than 100 users.

Step 16 Click **Apply** after entering all local user information. The user count is verified.

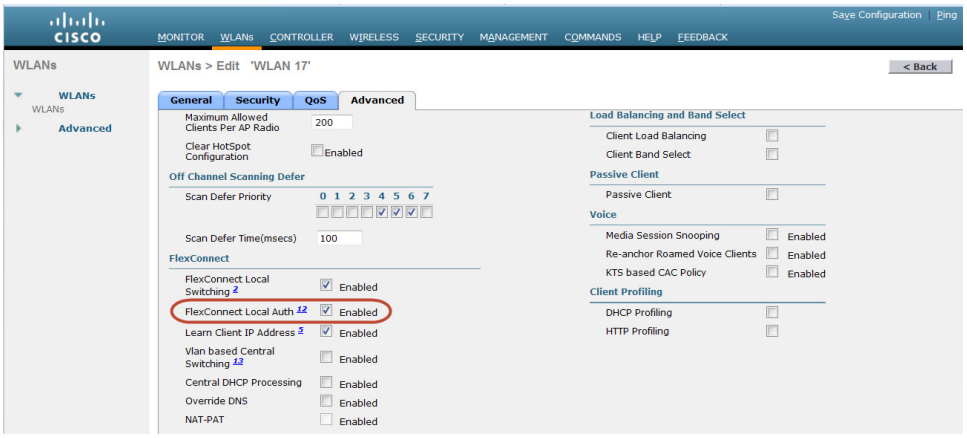


Step 17 From the top pane, click **WLANs**.

Step 18 Click WLAN ID number that was created during the AP Group creation. In this example, WLAN 17

Step 19 Under **WLAN > Edit for WLAN ID 17**, click **Advanced**.

Step 20 Check the **FlexConnect Local Auth** check box to enable Local Authentication in connected mode.



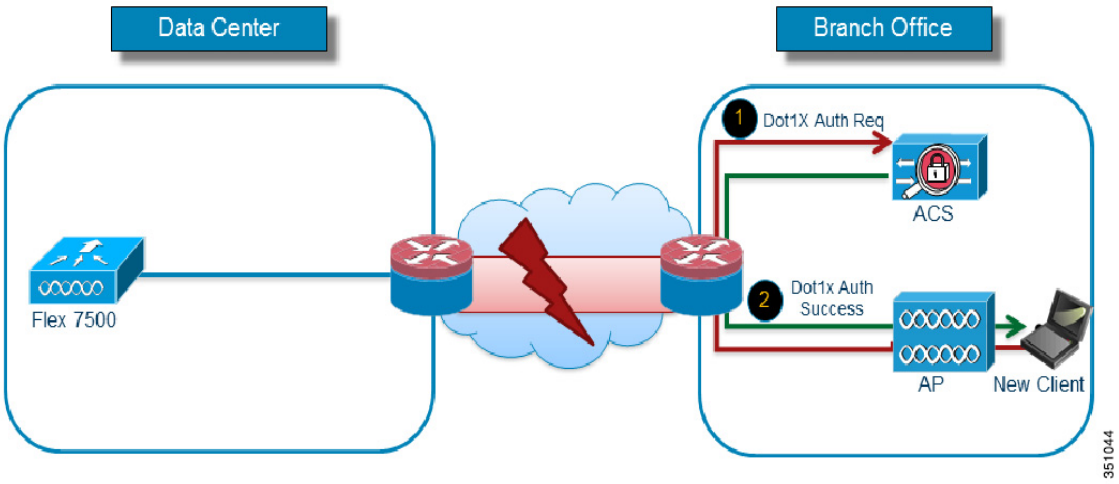
Note Local Authentication is supported only for FlexConnect with Local Switching. Always make sure to create the FlexConnect Group before enabling Local Authentication under WLAN

Local Authentication

Figure 7-8 illustrates clients continuing to perform 802.1X authentication even after the FlexConnect Branch APs lose connectivity with the controller. As long as the RADIUS/ACS server is reachable from the Branch site, wireless clients will continue to authenticate and access wireless services.

In other words, if the RADIUS/ACS is located inside the Branch, then clients will authenticate and access wireless services even during a WAN outage.

Figure 7-8 Local Authentication—AP Authenticator



- Configure Local Backup RADIUS server to increase the resiliency of the branch taking into consideration failures at the WAN, WLC failures, and failures at the RADIUS server.
- This feature is also used for remote offices where the WAN latency to the central site is high.
- Administrators can configure a primary backup RADIUS server or both the primary and secondary backup RADIUS server. FlexConnect AP in standalone mode can be configured to perform full 802.1X authentication to a backup RADIUS server.
- These servers are used when the FlexConnect AP is not connected to the controller or when the WLAN is configured for local authentication.
- If the RADIUS/ACS is located inside the branch, then the clients will authenticate and access wireless services even during a WAN outage.

Note When configuring local backup RADIUS server, note the following limitation: When a local backup RADIUS server is used in the branch, the IP addresses of all the APs acting as authenticators must be added on the RADIUS server.

Note The Local Authentication feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect Group is configured with both backup RADIUS server and local authentication, the FlexConnect AP 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 Local EAP Server on FlexConnect AP itself (if the primary and secondary are not reachable).

Local EAP

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

This feature is ideal for customers who are migrating from a standalone AP network to a lightweight FlexConnect AP 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 standalone AP.

Support for PEAP and EAP-TLS Authentication

FlexConnect AP can be configured as a RADIUS server for LEAP and EAP-FAST client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will do dot1x authentication on the AP itself using the local radius. With controller release 7.5, PEAP and EAP-TLS EAP methods are also supported.

CCKM/OKC Fast Roaming

FlexConnect Groups are required for Cisco's Centralized Key Management (CCKM) and Opportunistic Key Caching (OKC) fast roaming to work with FlexConnect APs. 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 AP.

This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one AP to another. The FlexConnect APs need to obtain the CCKM/OKC cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

For example, if you have a controller with 300 APs and 100 clients that might associate, sending the CCKM/OKC cache for all 100 clients may not be practical. If you create a FlexConnect Group comprising a limited number of APs (for example, you create a group for four APs in a remote office), the clients will then roam only among those four APs, and the CCKM/OKC cache is distributed among those four APs only when the clients associate to one of them.

This feature along with backup RADIUS and Local Authentication (Local-EAP) ensures no operational downtime for your branch sites.

Use FlexConnect groups in scenarios where CCKM/OKC fast roaming is required for clients when the FlexConnect AP is in connected or standalone mode.

This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one AP to another.

The FlexConnect APs need to obtain the CCKM/OKC cache information for all the clients that might associate so that they can process it quickly instead of sending it back to the controller.

Note CCKM/OKC fast roaming is supported on FlexConnect APs only.

FlexConnect VLAN Override

In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, and thus the client getting associated on a particular WLAN on a FlexConnect AP has to abide by a VLAN that is mapped to it. This method has limitations because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

From 7.2 release onwards, AAA override of VLAN on individual WLAN configured for local switching is supported. In order to have a dynamic VLAN assignment, APs would have the interfaces for the VLAN pre-created based on a configuration using existing WLAN-VLAN mapping for individual FlexConnect APs or using ACL-VLAN mapping on a FlexConnect group. The WLC is used to pre-create the sub-interfaces at the AP.

FlexConnect VLAN Override Summary

- AAA VLAN override is supported from release 7.2 for WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on WLANs configured for local switching.
- The FlexConnect AP should have VLAN pre-created from WLC for dynamic VLAN assignment.
- If VLANs returned by AAA override are not present on AP clients, they will get an IP from the default VLAN interface of the AP.

FlexConnect VLAN Based Central Switching

From release 7.3 onwards, traffic from FlexConnect APs can be switched centrally or locally depending on the presence of a VLAN on a FlexConnect AP.

In controller software release 7.2, AAA override of VLAN (Dynamic VLAN assignment) for locally-switched WLANs puts wireless clients on the VLAN provided by the AAA server. If the VLAN provided by the AAA server is not present at the AP, the client is put on a WLAN mapped VLAN on that AP and traffic switches locally on that VLAN. Further, prior to release 7.3, traffic for a particular WLAN from FlexConnect APs can be switched Centrally or Locally depending on the WLAN configuration.

FlexConnect VLAN Central Switching Summary

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in connected mode are as follows:

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally and the client is assigned this VLAN/Interface returned from the AAA server provided that the VLAN exists on the WLC.

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the FlexConnect AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be assigned a VLAN/Interface mapped to a WLAN on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client is assigned a WLAN mapped VLAN on that FlexConnect AP and traffic is switched locally.

Traffic flow on WLANs configured for Local Switching when FlexConnect APs are in standalone mode are as follows:

- If the VLAN returned by the AAA server is not present in the FlexConnect AP database, the client will be put on a default VLAN (that is, a WLAN mapped VLAN on a FlexConnect AP). When the AP connects back, this client is de-authenticated and will switch traffic centrally.
- If the VLAN returned by the AAA server is present in the FlexConnect AP database, the client is placed into a returned VLAN and traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client is assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

VLAN Name Override

The VLAN Name Override feature is useful in deployments that have a single central radius authenticating multiple branches. With hundreds of different branches, it becomes very difficult to standardize VLAN IDs across all sites and requires a configuration that provides a unique VLAN Name mapped locally to a VLAN ID that can be different across different branch locations.

This design involving different VLAN IDs across different sites is also useful from the sizing and scaling perspective to limit the number of clients per Layer 2 broadcast domain.

FlexConnect VLAN Name Override Summary

- The VLAN Name Override feature supports both Central and Local Authentication with local switching WLANs.
- If the AAA server returns multiple VLAN attributes, preference is given to the VLAN Name attribute.
- When Aire-Interface-Name and Tunnel-Private-Group-ID are both returned, the Tunnel-Private-Group-ID attribute is given preference.
- If AAA server returns an unknown VLAN name attribute, the client is defaulted to the WLAN-VLAN ID mapping present on the AP.
- This feature is also supported in the standalone mode.

FlexConnect ACL

With the introduction of ACLs on FlexConnect, there is a mechanism to cater to the need of access control at the FlexConnect AP for protection and integrity of locally-switched data traffic from the AP. FlexConnect ACLs are created on the WLC and should then be configured with the VLAN present on the FlexConnect AP or FlexConnect group using VLAN-ACL mapping, which will be for AAA override VLANs. These are then pushed to the AP.

FlexConnect ACL Summary

- Create FlexConnect ACL on the controller.
- Apply the same on a VLAN present on FlexConnect AP under AP Level VLAN ACL mapping.
- Can be applied on a VLAN present in FlexConnect Group under VLAN-ACL mapping (generally done for AAA overridden VLANs.
- While applying ACL on VLAN, select the direction to be applied: *ingress*, *egress*, or *ingress and egress*.

FlexConnect ACL Limitations

- A maximum of 512 FlexConnect ACLs can be configured on WLC.
- Each individual ACL can be configured with 64 rules.
- A maximum of 32 ACLs can be mapped per FlexConnect group or per FlexConnect AP.
- At any given point in time, there is a maximum of 16 VLANs and 32 ACLs on the FlexConnect AP.

Client ACL Support

Prior to release 7.5, FlexConnect ACLs are supported on the VLAN. Also, AAA override of VLANs is supported. If a client gets an AAA override of VLAN, it is placed on the overridden VLAN and the ACL on the VLAN applies for the client. If an ACL is received from the AAA for locally switched clients, it is ignored. With release 7.5, this limitation is addressed and the support for client based ACLs for locally switched WLANs is provided.

FlexConnect Split Tunneling

Split Tunneling introduces a mechanism by which the traffic sent by the client will be classified, based on packet content, using FlexConnect ACL. Matching packets are switched locally from FlexConnect AP and the rest of the packets are centrally-switched over CAPWAP.

The Split Tunneling functionality is an added advantage for OEAP setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly without consuming WAN bandwidth by sending packets over CAPWAP.

FlexConnect ACL can be created with rules in order to permit all of the devices present at the local site/network. When packets from a wireless client on the Corporate SSID match the rules in the FlexConnect ACL configured on OEAP, that traffic is switched locally and the rest of the traffic (that is, implicit deny traffic) will switch centrally over CAPWAP.

The Split Tunneling solution assumes that the subnet/VLAN associated with a client in the central site is not present in the local site (that is, traffic for clients that receive an IP address from the subnet present on the central site will not be able to switch locally).

The Split Tunneling functionality is designed to switch traffic locally for subnets that belong to the local site in order to avoid WAN bandwidth consumption. Traffic that matches the FlexConnect ACL rules are switched locally, and NAT operation is performed changing the client's source IP address to the FlexConnect AP's interface IP address that is route-able at the local site/network.

Split Tunnel Summary

- The Split Tunneling functionality is supported on WLANs configured for central switching advertised by FlexConnect APs only.
- The DHCP required should be enabled on WLANs configured for Split Tunneling.
- The Split Tunneling configuration is applied per WLAN configured for central switching on a per FlexConnect AP basis or for all of the FlexConnect APs in a FlexConnect Group.

Split Tunnel Limitations

- FlexConnect ACL rules should not be configured with permit/deny statement with same subnet as source and destination.
- Traffic on a centrally-switched WLAN configured for Split Tunneling can be switched locally only when a wireless client initiates traffic for a host present on the local site. If traffic is initiated by clients/host on a local site for wireless clients on these configured WLANs, the traffic will not be able to reach the destination.
- Split Tunneling is not supported for Multicast/Broadcast traffic. Multicast/Broadcast traffic will switch centrally even if it matches the FlexConnect ACL.
- Split tunnel feature is not supported in a foreign anchor roaming scenario

Fault Tolerance

FlexConnect fault tolerance allows wireless access and services to branch clients when the FlexConnect Branch APs:

- Lose connectivity with the primary controller.
- Are switching to the secondary controller.
- Are re-establishing connection to the primary controller.

FlexConnect fault tolerance, along with the local EAP, provides zero branch downtime during a network outage. This feature is enabled by default and cannot be disabled. It requires no configuration on the controller or AP. However, to ensure fault tolerance works smoothly and is applicable, these criteria should be maintained:

- WLAN ordering and configurations have to be identical across the primary and backup controllers.

- VLAN mapping has to be identical across the primary and backup controllers.
- Mobility domain name has to be identical across the primary and backup controllers.
- Use FlexConnect 7500 as both the primary and backup controllers.

Fault Tolerance Summary

- FlexConnect will not disconnect clients when the AP is connecting back to the same controller provided there is no change in configuration on the controller.
- FlexConnect will not disconnect clients when connecting to the backup controller provided there is no change in configuration and the backup controller is identical to the primary controller.
- FlexConnect will not reset its radios on connecting back to the primary controller provided there is no change in configuration on the controller.

Fault Tolerance Limitations

- Supported only for FlexConnect with Central/Local Authentication with Local Switching.
- Centrally-authenticated clients require full re-authentication if the client session timer expires before the FlexConnect AP switches from standalone to connected mode.
- The primary and backup controllers must be in the same mobility domain.

Peer-to-Peer Blocking

Peer-to-peer (P2P) blocking is supported for clients associated on local switching WLAN. Per WLAN, peer-to-peer configuration is pushed by the controller to the FlexConnect AP. P2P blocking can be configured on a WLAN with any of these three actions:

- Disabled—Disables P2P blocking and bridged traffic locally, within the controller, for clients in the same subnet. This is the default value.
- Drop—This causes the controller to discard packets for clients in the same subnet.
- Forward Up-Stream—This forwards a packet on the upstream VLAN. The devices above the controller decide what action to take regarding the packet.

P2P Summary

- P2P Blocking is configured per WLAN.
- Per WLAN, P2P blocking configuration is pushed by the WLC to FlexConnect APs.
- P2P blocking action configured as drop or upstream-forward on a WLAN is treated as P2P blocking enabled on the FlexConnect AP.

P2P Limitations

- In FlexConnect solution, P2P blocking configuration cannot be applied only to a particular FlexConnect.

- AP or subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports P2P upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as P2P drop, and client packets are dropped instead of forwarded to the next network node.
- Unified solution for central switching clients supports P2P blocking for clients associated to different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a work around for this limitation.

FlexConnect WGB/uWGB Support for Local Switching WLANs

From release 7.3 onward, Cisco's Work Group Bridge/Universal Work Group Bridge (WGB/uWGB) and wired/wireless clients behind WGBs are supported and will work as normal clients on WLANs configured for local switching.

After association, WGB sends the IAPP messages for each of its wired/wireless clients, and FlexConnect APs behave as follows:

- When a FlexConnect AP is in connected mode, it forwards all the IAPP messages to the controller and the controller will process the IAPP messages the same as of local mode AP. Traffic for wired/wireless clients is switched locally from FlexConnect APs.
- An AP in standalone mode processes the IAPP messages; wired/wireless clients on the WGB must be able to register and de-register. Upon transition to connected mode, FlexConnect AP sends the information of wired clients back to the controller. WGB will send registration messages three times when FlexConnect AP transitions from standalone to connected mode.

  Wired/Wireless clients will inherit the WGB's configuration, which means no separate configuration like AAA authentication, AAA override, and FlexConnect ACL is required for clients behind WGB.

FlexConnect WGB/uWGB Summary

- No special configuration is required on WLC in order to support WGB on FlexConnect AP.
- Fault Tolerance is supported for WGB and the clients behind WGB.
- WGB is supported on an IOS AP: 1240, 1130, 1140, 1260, and 1250.

FlexConnect WGB/uWGB Limitations

- Wired clients behind WGB will always be on the same VLAN as WGN itself. Multiple VLAN support for clients behind WGB is not supported on the FlexConnect AP for WLANs configured for local switching.
- A maximum of 20 clients (wired/wireless) is supported behind WGB when associated to FlexConnect AP on WLAN configured for local switching.
- WebAuth is not supported for clients behind WGB associated on WLANs configured for local switching.

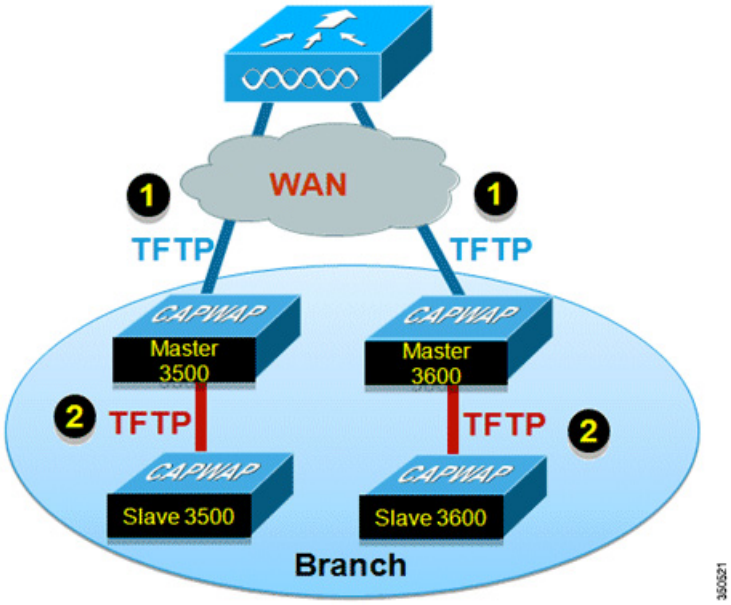
FlexConnect Smart AP Image Upgrade

The pre-image download feature reduces the downtime duration to a certain extent, but still all the FlexConnect APs have to pre-download the respective AP images over the WAN link with higher latency.

Efficient AP Image Upgrade will reduce the downtime for each FlexConnect AP. The basic idea is only one AP of each AP model will download the image from the controller and will act as Master/Server, and the rest of the APs of the same model will work as Slave/Client and will pre-download the AP image from the master.

The distribution of AP image from the server to the client will be on a local network and will not experience the latency of the WAN link. As a result, the process will be faster.

Figure 7-9 Smart AP Image Upgrade



Smart AP Image Upgrade Summary

- Master and Slave APs are selected for each AP model per FlexConnect Group.
- Master downloads image from WLC.
- Slave downloads image from Master AP.
- Reduces downtime and saves WAN bandwidth.

VideoStream for FlexConnect Local Switching

Release 8.0 introduces VideoStream for Local Switching feature, for branch office deployments.

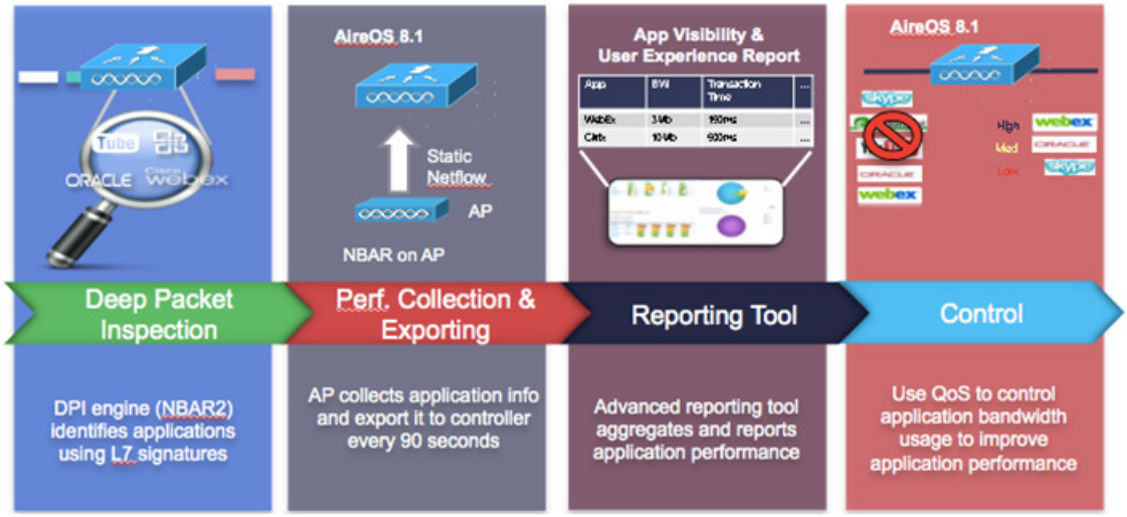
This feature enables the wireless architecture to deploy multicast video streaming across the branches, as it is currently possible for enterprise deployments.

This feature recompenses the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

Application Visibility and Control for FlexConnect

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and WLC platforms. The support of AVC embedded within the FlexConnect AP extends, as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

Figure 7-10 Application Visibility and Control for FlexConnect



- NBAR2 engine runs on the FlexConnect AP.
- Classification of applications happens at the access point using the DPI engine (NBAR2) to identify applications using L7 signatures.
- AP collects application information and exports it to controller every 90 seconds.
- Real-time applications are monitored on the controller user interface.
- Ability to take actions, drop, mark or rate-limit, is possible on any classified application on the FlexConnect access point.

AVC Facts and Limitations

- AVC on the FlexConnect AP can classify and take action on 1000+ different applications.
- The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- Intra FlexConnect Group roaming support.

- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- Multicast traffic is not supported by AVC application.
- Netflow export for FlexConnect AVC is not supported in 8.1.

General Deployment Considerations

- Although it is possible for any WLC to support FlexConnect APs, depending on the number of branch locations and subsequently the total number of APs being deployed, it makes sense (from an administrative standpoint) to consider using a dedicated WLC(s) to support a FlexConnect deployment.
- FlexConnect APs typically do not share the same policies as APs within a main campus; each branch location is essentially an RF and mobility domain unto itself. Even though a single WLC cannot be partitioned into multiple logical RF and mobility domains, a dedicated WLC allows branch-specific configuration and policies to be logically separate from the campus.
- If deployed, a dedicated FlexConnect WLC should be configured with a different mobility and RF network name than that of the main campus. All FlexConnect APs joined to the dedicated WLC become members of that RF and mobility domain.
- From an auto-RF standpoint, assuming there are enough FlexConnect APs deployed within a given branch, the WLC attempts to auto manage the RF coverage associated with each branch.
- There is no advantage (or disadvantage) in having the FlexConnect APs consolidated into their own mobility domain. This is because client traffic is switched locally. EoIP mobility tunnels are not invoked between WLCs (of the same mobility domain) where client roaming with FlexConnect APs is involved.
- If a dedicated WLC is going to be used for a FlexConnect deployment, a backup WLC should also be deployed to ensure network availability. As with standard AP deployments, the WLC priority should be set on the FlexConnect APs to force association with the designated WLCs.
- Certain architectural requirements need to be considered when deploying a distributed branch office in terms of the Minimum WAN Bandwidth, Maximum RTT, Minimum MTU, and fragmentation.
- Check to make sure that the AP model being used has FlexConnect support. The AP model OEAP600 does not support FlexConnect mode.
- Set QoS to prioritize CAPWAP Control Channel traffic on UDP port 5246.
- You can deploy a FlexConnect AP with either a static IP address or a DHCP address. A DHCP server must be available locally and must be able to provide the IP address for the AP during boot-up.
- FlexConnect supports up to four fragmented packets or a minimum 500 byte maximum transmission unit (MTU) WAN link.
- Round-trip latency must not exceed 300 milliseconds (ms) between the AP and the controller. If the 300 milliseconds round-trip latency cannot be achieved, configure the AP to perform local authentication.
- FlexConnect includes robust fault tolerance methodology. When the AP and the controller have the same configuration, the connections (rejoin or standby) between the clients and the FlexConnect APs are maintained intact and the clients experience seamless connectivity.

- The primary and secondary controllers for a FlexConnect AP must have the same configuration. Otherwise, the AP might lose its configuration, and certain features (such as WLAN overrides, VLANs, static channel number, and so on) may not operate as expected. In addition, make sure to duplicate the SSID of the FlexConnect AP and its index number on both controllers.
- Client connections are restored only for locally-switched clients that are in the RUN state when the AP moves from standalone mode to connected mode. After the AP moves from the standalone mode to the connected mode, the AP's radio is also reset.
- Session time-out and re-authentication are performed when the AP establishes a connection to the controller.
- If a session timer expires, the client user name, current/support rate, and listen interval values are reset to the default values. When the client connection is re-established, the controller does not restore the client's original attributes.
- Multiple FlexConnect groups can be defined in a single location. There is no deployment restriction on the number of FlexConnect APs per location.
- In FlexConnect mode, the AP can receive multicast packets only in unicast form.
- FlexConnect APs support a 1-1 network address translation (NAT) configuration and a port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the unicast option. FlexConnect APs 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 APs, 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 AP.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported on WLANs configured for FlexConnect local switching.
- Workgroup bridges and universal workgroup bridges are supported on FlexConnect APs for locally-switched clients.
- FlexConnect APs do not support client load balancing.
- FlexConnect supports IPv6 clients by bridging the traffic to a local VLAN, similar to IPv4 operation.
- FlexConnect does not support IPv6 ACLs, neighbor discovery caching, or DHCPv6 snooping of IPv6 NDP packets.
- FlexConnect APs with locally-switched WLANs cannot perform IP Source Guard and prevent ARP spoofing. For centrally-switched WLANs, the wireless controller performs the IP Source Guard and ARP Spoofing. To prevent ARP spoofing attacks in FlexConnect APs with local switching, Cisco recommends you to use ARP inspection.