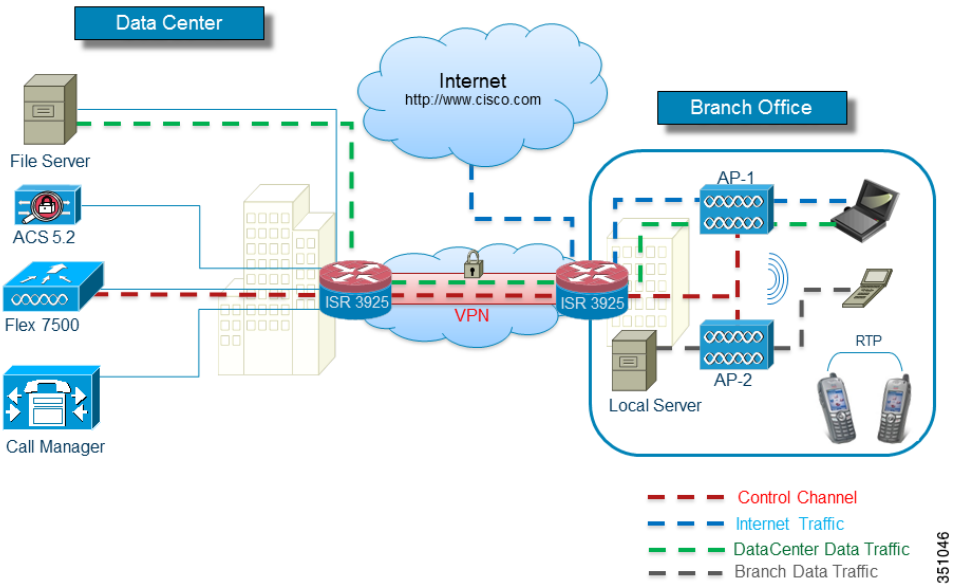
FlexConnect

FlexConnect（以前は、ハイブリッド リモート エッジ アクセス ポイントまたは H-REAP と呼ばれていました）は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。これにより、各オフィスにコントローラを導入することなく、ブランチ オフィスやリモート オフィスにあるアクセス ポイント（AP）を、本社オフィスからワイドエリア ネットワーク（WAN）リンク経由で設定して制御できます。FlexConnect アクセス ポイント（AP）は、クライアント データ トラフィックをローカルに切り替え、クライアント認証をローカルに実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

図 7-1　　FlexConnect のアーキテクチャ



（注）　FlexConnect 機能マトリクスについては、http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b3690b.shtml#matrix を参照してください。

サポートされるプラットフォーム

FlexConnect は、次のコンポーネントでのみサポートされます。

- 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 アクセス ポイント
- 1815i、1815W、1815-OEAP、1540 1560 レガシー AP:3500、OEAP 600、3600、2600、1600、3700、2700、1700、702、702W、802、1530、1552WU、1550、1570、1800 シリーズ、2800 シリーズ、3800 シリーズ
- Cisco 5520、8540、Flex 7500、Cisco 8500、4400、5500、3504、2500 シリーズ コントローラ
- Cisco WiSM-2
- Cisco 仮想コントローラ（vWLC）

FlexConnect の用語

わかりやすくするために、ここではこの章全体で使用される FlexConnect の用語と定義について、概要を説明します。

スイッチング モード

FlexConnect AP は、WLAN ごとに次のスイッチング モードを同時にサポートできます。

ローカル スイッチング

ローカル スイッチング WLAN は、802.1Q トランキング経由で、別個の VLAN（隣接するルータまたはスイッチのいずれか）にワイヤレス ユーザ トラフィックをマップします。必要に応じて、1 つ以上の WLAN を同じローカル 802.1Q VLAN にマップできます。

ローカル スイッチング WLAN にアソシエートされたブランチ ユーザは、オンサイト ルータによってトラフィックが転送されます。オフサイト（セントラル サイト）に送信されるトラフィックは、ブランチ ルータによって、標準の IP パケットとして転送されます。AP の制御および管理に関連するすべてのトラフィックは、Control and Provisioning of Wireless Access Points（CAPWAP）プロトコル経由で、中央集中型ワイヤレス LAN コントローラ（WLC）に個別に送信されます。

中央スイッチング

中央スイッチング WLAN は、CAPWAP 経由で、ワイヤレス ユーザ トラフィックと制御トラフィックの両方を中央集中型 WLC にトンネリングします。ここで、ユーザ トラフィックは WLC 上のダイナミック インターフェイスまたは VLAN にマップされます。これは、CAPWAP モードの通常の動作です。

中央スイッチング WLAN にアソシエートされたブランチ ユーザのトラフィックは、中央集中型 WLC に直接トンネリングされます。そのユーザが（そのクライアントがアソシエートされた）ブランチ内部のコンピューティング リソースと通信する必要がある場合、そのユーザのデータは WAN リンクを介して、標準 IP パケットとしてブランチ ロケーションに戻されます。WAN リンクの帯域幅によっては、望ましい動作が得られない場合があります。

動作モード

FlexConnect AP には、次の 2 種類の動作モードがあります。

接続モード:WLC に到達可能な状態です。このモードでは、FlexConnect AP とその WLC が CAPWAP 接続されます。

スタンドアロン モード:WLC に到達できない状態です。FlexConnect はその WLC との CAPWAP 接続を失ったか、または確立に失敗しました。この状態は、ブランチ サイトとセントラル サイト間の WAN リンクが停止した場合などに発生します。

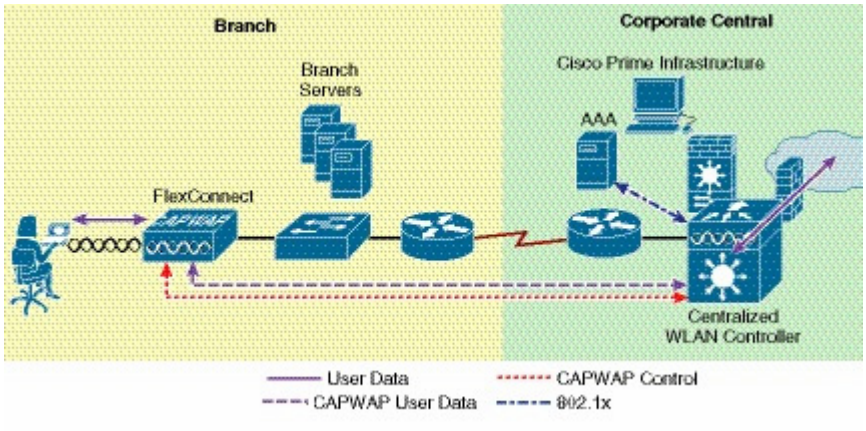
FlexConnect の状態

FlexConnect WLAN は、その構成とネットワーク接続によって、次のいずれかの状態に分類されます。

中央認証/中央スイッチング

WLAN が、802.1X、VPN、または Web などの中央集中型認証方式を使用している状態です。ユーザ トラフィックは CAPWAP 経由で WLC に送信されます。この状態は、FlexConnect が接続モードの場合にのみサポートされます(図 7-2 を参照)。この例では 802.1X が使用されていますが、他のメカニズムにも同様に適用できます。

図 7-2　中央認証/中央スイッチング WLAN



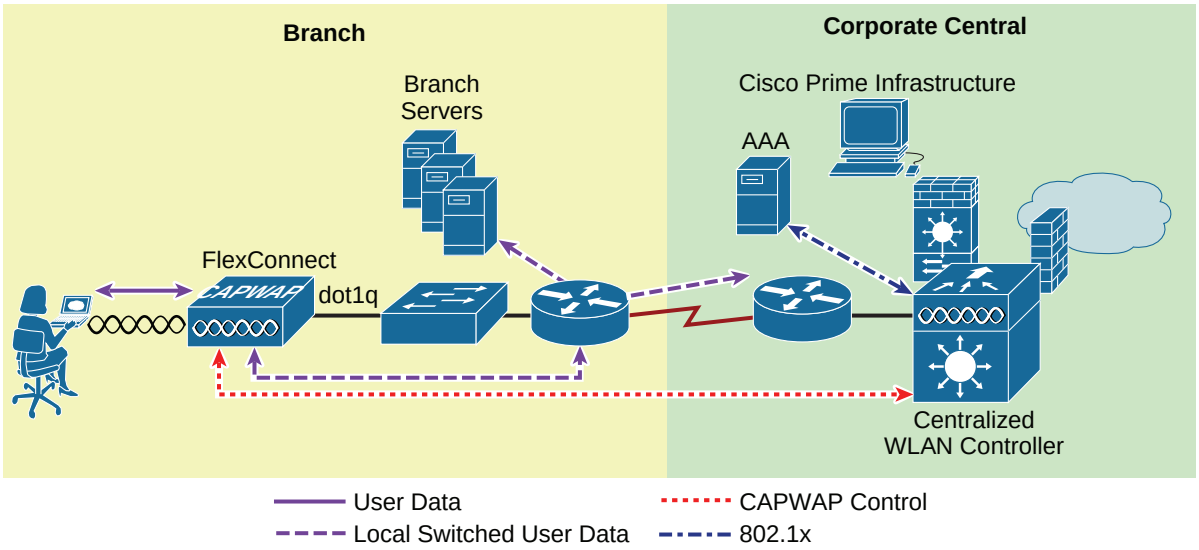
認証ダウン/スイッチング ダウン

FlexConnect AP がスタンドアロン モードのときは、中央スイッチング WLAN(上記)がプローブ要求に対してビーコンを送ったり、応答したりすることはありません。既存のクライアントのアソシエーションは解除されます。

中央認証/ローカル スイッチング

WLAN は中央集中型認証を使用しますが、ユーザ トラフィックがローカルにスイッチングされる状態です。この状態は、FlexConnect AP が接続モードの場合にのみサポートされます（図 7-3 を参照）。図 7-3 の例では 802.1X が使用されていますが、他のメカニズムにも同様に適用できます。

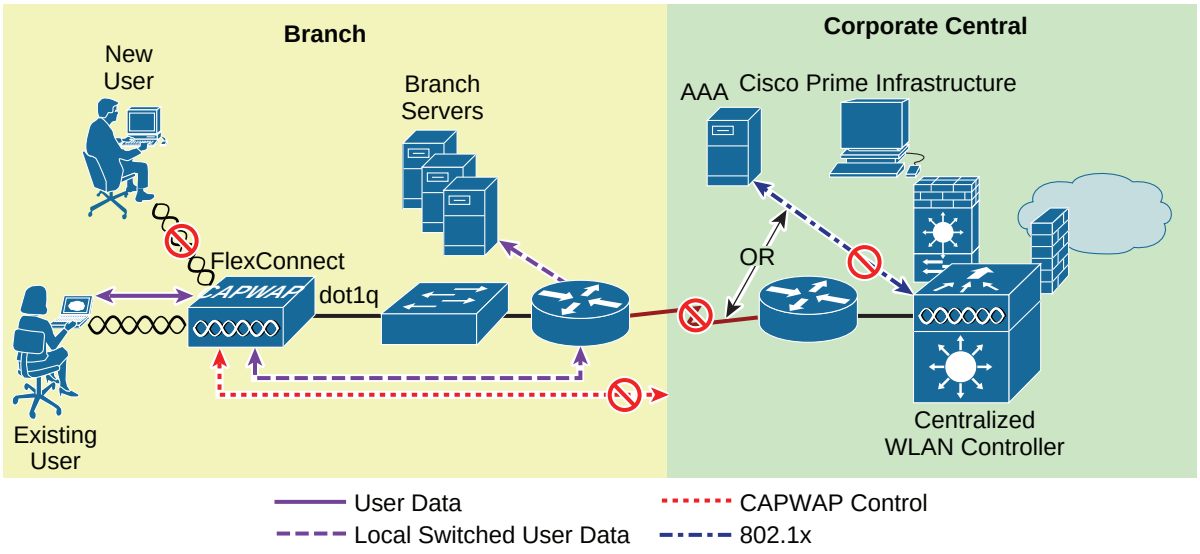
図 7-3　中央認証/ローカル スイッチング WLAN



認証ダウン/ローカル スイッチング

中央集中型認証を必要とする WLAN（上述のとおり）は、新しいユーザを拒否します。すでに認証済みのユーザは、セッションのタイムアウトまで、引き続きローカルにスイッチングされます（セッションのタイムアウトが設定されている場合）。WLAN にアソシエートされている（既存の）ユーザがなくなるまで、WLAN はビーコン送信およびプローブ応答を継続します。この状態は、AP がスタンドアロン モードに移行した結果として発生します（図 7-4）。

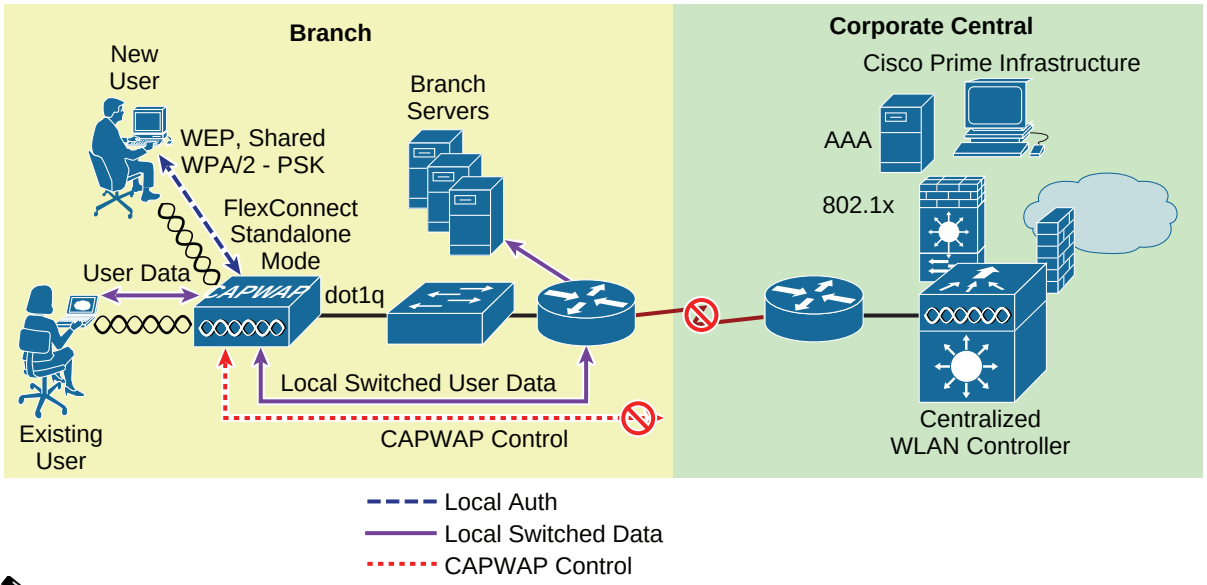
図 7-4　認証ダウン/ローカル スイッチング



ローカル認証/ローカル スイッチング

WLAN がオープンなセキュリティ方式、スタティック WEP、共有型セキュリティ方式、または WPA2 PSK セキュリティ方式を使用している状態です。ユーザ トラフィックはローカルにスイッチングされます。FlexConnect がスタンドアロン モードになると、これらのセキュリティ方式だけがローカルにサポートされます。WLAN は、ビーコン送信およびプローブ応答を継続します（図 7-5 を参照）。既存のユーザは接続されたままで、新しいユーザのアソシエーションが受け入れられます。AP が接続モードの場合、これらのセキュリティ タイプの認証情報は WLC に転送されます。

図 7-5　ローカル認証/ローカル スイッチング WLAN



（注）　AP がどの動作モードにあるかに関係なく、すべての 802.11 認証およびアソシエーション処理が発生します。接続モードのときは、FlexConnect AP はすべてのアソシエーション/認証情報を WLC に転送します。スタンドアロン モードのときは、AP はこれらのイベントを WLC に通知することができません。そのため、中央集中型認証/スイッチング方式を使用する WLAN は使用できなくなります。

アプリケーション

FlexConnect AP は、次のように、きわめて柔軟な展開が可能です。

- ブランチのワイヤレス接続
- ブランチのゲスト アクセス
- WLAN 公共ホットスポット
- ブランチ サイトでのワイヤレス BYOD

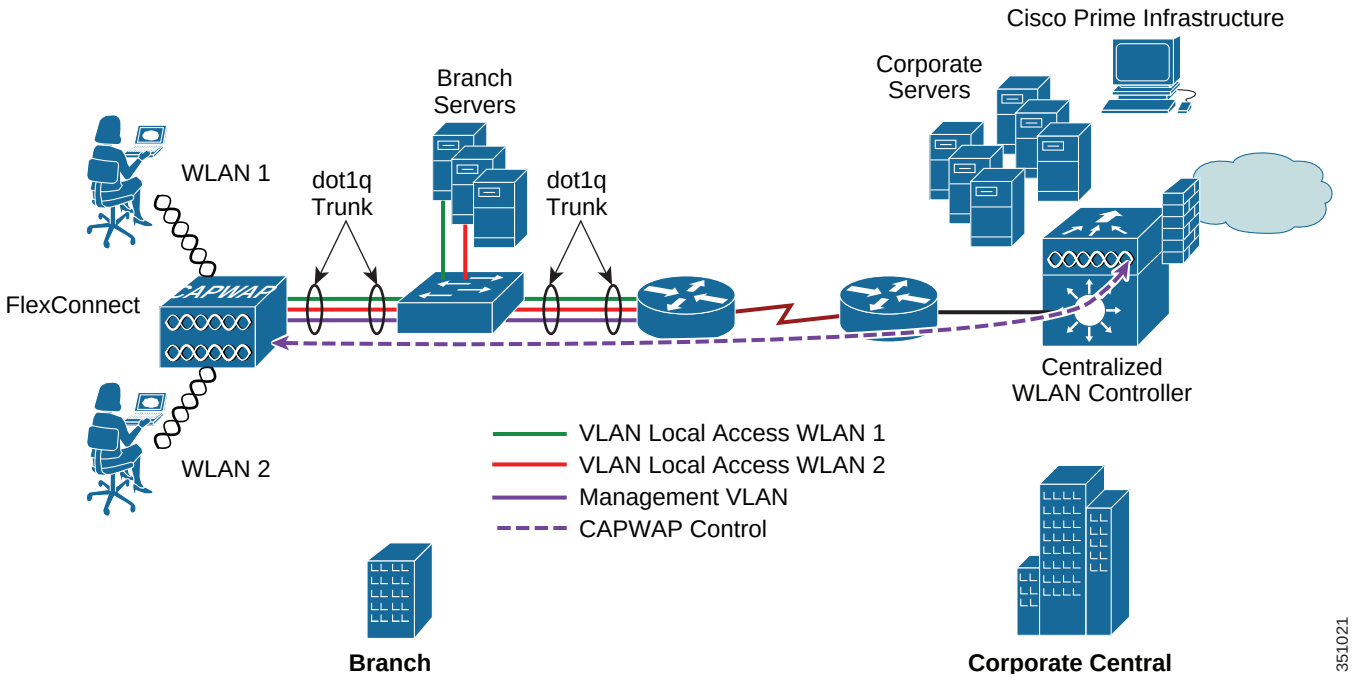
ブランチのワイヤレス接続

FlexConnect は、ワイヤレス ユーザ トラフィックを WAN 経由で中央の WLC にトンネリングするのではなく、ローカルに終了できるようにすることで、ブランチ ロケーションのワイヤレス接続のニーズに対応します。FlexConnect により、ブランチ ロケーションでは図 7-6 に示すように、WLAN ごとにセグメンテーション、アクセス制御、および QoS ポリシーをより効果的に実装できます。

ブランチのゲスト アクセス

中央集中型 WLC 自身が、図 7-6 に示すように、ゲスト アクセス WLAN に対して Web ネットワーク認証を実行できます。ゲスト ユーザのトラフィックは、他のブランチ オフィスのトラフィックから分割（隔離）されます。ゲスト アクセスの詳細については、第 10 章「Cisco Unified Wireless Network ゲスト アクセス サービス」を参照してください。

図 7-6　FlexConnect トポロジ

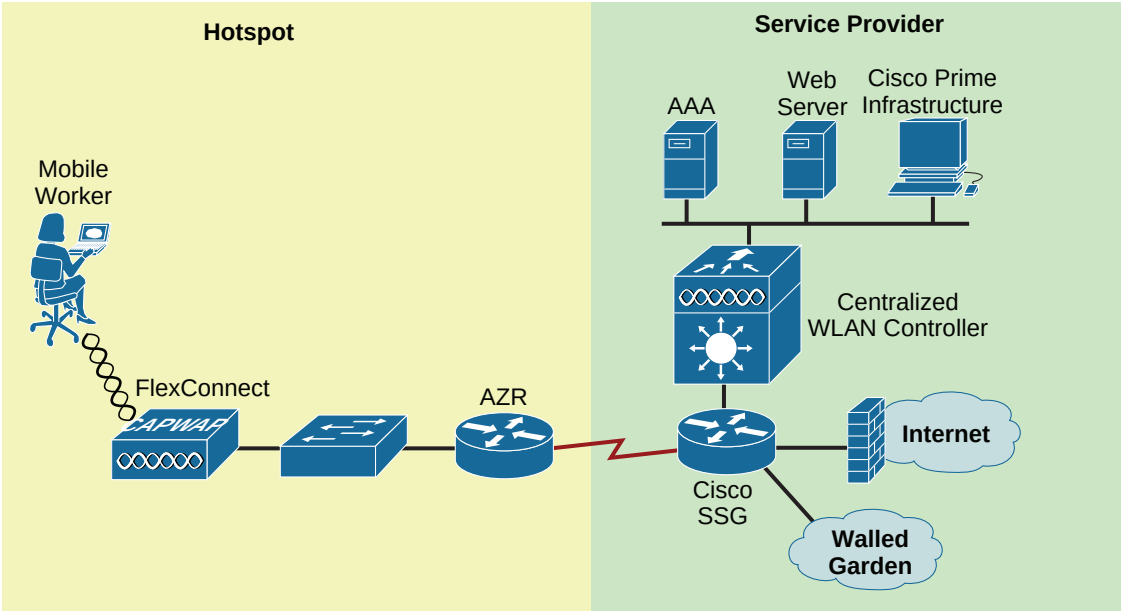


WLAN 公共ホットスポット

多くの公共ホットスポット サービス プロバイダーは、複数の SSID/WLAN の実装を始めています。この理由の 1 つは、Web ベースのアクセス用のオープン認証 WLAN と、これとは別に、より安全なパブリック アクセス用に 802.1x/EAP を使用する WLAN も提供したいと考える事業者も存在するためです。

WLAN を個別の VLAN にマップできる FlexConnect AP は、1、2 個の AP しか必要としない小規模地域のホットスポット展開で、スタンドアロン AP の代替手段となります。図 7-7 は、FlexConnect AP を使用したホットスポット トポロジの例を示しています。

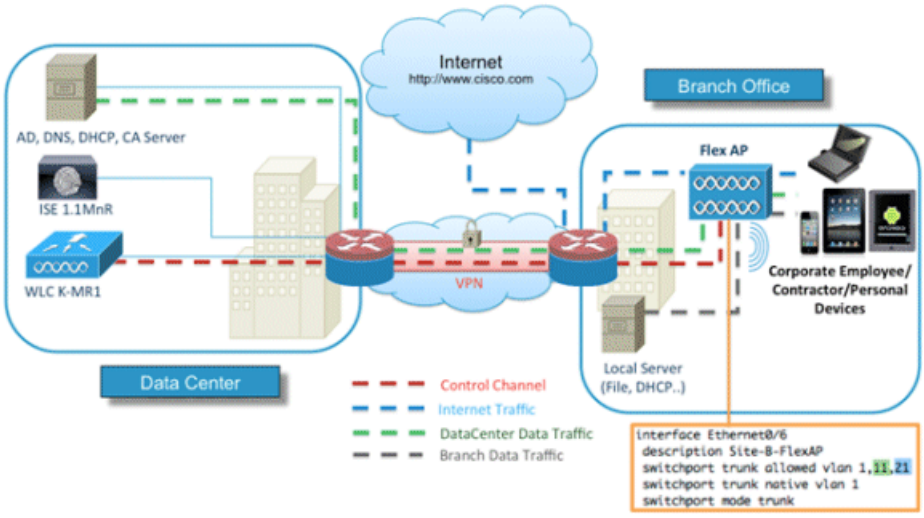
図 7-7　FlexConnect ローカル スイッチングを使用したホットスポット アクセス



ブランチ サイトでのワイヤレス BYOD

リリース 7.2.110.0 は、ローカルにスイッチングされ、中央で認証されるクライアントに対し、FlexConnect AP の ISE 機能をサポートします。また、リリース 7.2.110.0 は ISE 1.1.1 と統合されているため、ワイヤレス環境において、たとえば以下のような BYOD ソリューションを提供します。

- デバイスのプロファイリングとポスチャ
- デバイスの登録とサプリカントのプロビジョニング
- 個人用デバイスのオンボード（iOS または Android デバイスのプロビジョニング）



構成の考慮事項

ここでは、FlexConnect AP の導入に関するさまざまな実装と運用上の注意について説明します。

WAN リンク

FlexConnect AP を予測どおりに機能させるためには、WAN リンク特性に関する次のことに留意してください。

- 遅延：特定の WAN リンクで 100 ミリ秒を超える遅延が発生しないように管理する必要があります。AP は、30 秒ごとにハートビート メッセージを WLC に送信します。ハートビート応答がない場合、AP は 5 回連続（1 秒に 1 回ずつ）でハートビート メッセージを送信して、まだ接続しているかどうかを確認します。接続が失われている場合は、FlexConnect AP はスタンドアロン モードに切り替わります。

  同様に、AP と WLC はエコー CAPWAP パケットを交換して、接続の有無を確認します。エコー CAPWAP パケットの応答がない場合、AP は 5 回連続（3 秒に 1 回ずつ）でエコー CAPWAP パケットを送信して、まだ接続しているかどうかを確認します。接続が失われている場合は、FlexConnect AP はスタンドアロン モードに切り替わります（動作モードの定義については動作モード（7-3 ページ）を参照）。AP 自体は、比較的高い遅延耐性を持っています。ただし、クライアントでは、認証に関連付けられたタイマーはリンク遅延に対して敏感であり、100 ミリ秒未満の制約が要求されます。遅延がそれ以上になると、クライアントは認証を待機しながらタイムアウトとなる可能性があり、この結果、ルーピングなど、その他の予測不可能な動作が発生するおそれがあります。

- 帯域幅：1 つのロケーションに 8 ヵ所以下の AP を展開する場合は、WAN リンクに 128 kbps 以上の帯域幅が必要です。8 ヵ所を超える AP を展開する場合、比例配分により高い帯域幅を WAN リンクにプロビジョニングする必要があります。

- パス MTU：500 バイト以上の MTU が必要です。

ローミング

FlexConnect AP が接続モードのときは、すべてのクライアント プローブ、アソシエーション要求、802.1x 認証要求、および対応する応答メッセージが、CAPWAP コントロール プレーンを経由して AP と WLC の間で交換されます。これは、オープン、スタティック WEP、および WPA PSK ベースの WLAN にも当てはまります。AP がスタンドアロン モードのときは、これらの認証方式を使用するために CAPWAP 接続を必要としませんが、その場合も同様です。

- ダイナミック WEP/WPA：これらのキー管理方式のいずれかを使用して FlexConnect AP 間をローミングするクライアントは、ローミングするたびに完全な認証を実行します。認証が成功すると、新しいキーが AP とクライアントに渡されます。この動作は、標準の中央集中型 WLAN 展開と同じです。ただし、FlexConnect トポロジ内では、WAN 全体でさまざまなリンク遅延が生じることがあり、この結果、合計ローミング時間に影響が及ぶ可能性があります。使用されている WAN の特性、RF 設計、バック エンド認証ネットワーク、および認証プロトコルに応じて、ローミング時間が変動する場合があります。

- WPA2：クライアントのローミング時間を短縮するために、WPA2 では、IEEE 802.11i 仕様に基づくキー キャッシング機能を導入しています。シスコでは、この仕様に Proactive Key Caching（PKC）と呼ばれる拡張機能を追加しました。現在、PKC は Microsoft の Zero Config Wireless サプリカントと Funk（Juniper）Odyssey クライアントでのみサポートされています。Cisco CCKM も WPA2 と互換性があります。

ワイヤレス IP テレフォニーなどのアプリケーションをサポートする、予測可能な高速ローミングの動作が必要となるリモート ブランチ ロケーションでは、ローカル WLC（UCS ブレード上の仮想コントローラ、または 2500 WLC）の導入を検討する必要があります。

- Cisco Centralized Key Management（CCKM）：CCKM はシスコが開発したプロトコルです。このプロトコルでは、CCKM 対応クライアントのセキュリティ クレデンシャルが WLC にキャッシュされ、モビリティ グループ内の他の AP に転送されます。クライアントが他の AP にローミングおよびアソシエートするとき、クレデンシャルがこの AP に転送されるため、2 段階プロセスでクライアントを再びアソシエートして認証できます。これにより、AAA サーバでの完全認証を実行する必要がなくなります。CCKM 対応クライアントは、ある FlexConnect から別の FlexConnect に移動するたびに、完全な 802.1x 認証を受けます。
- CCKM/OKC 高速ローミングで FlexConnect アクセス ポイントを使用するには、FlexConnect グループが必要となります。高速ローミングは、完全な EAP 認証で使用されたマスター キーの派生キーをキャッシュすることにより実現します。これにより、ワイヤレス クライアントが別のアクセス ポイントにローミングする際に、簡単かつ安全にキー交換できるようになります。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。しかし、たとえば 300 のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対する CCKM/OKC キャッシュを送信することは現実的ではありません。限定した数のアクセス ポイントから成る FlexConnect グループを作成すれば（たとえば、1 つのリモート オフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM/OKC キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがそのいずれかにアソシエートするときだけとなります。
- レイヤ 2 スイッチの CAM テーブルの更新：クライアントがローカルにスイッチングされる WLAN 上で、ある AP から別の AP にローミングしたときに、FlexConnect はクライアントがポートを変更したことをレイヤ 2 スイッチに通知しません。スイッチは、クライアントがデフォルト ルータに対する ARP 要求を実行するまで、クライアントがローミングしたことを認識しません。この動作は、わずかですが、ローミングのパフォーマンスに影響を与える可能性があります。

（注）　（所定のローカル スイッチング WLAN 上で）WLAN を異なる VLAN/サブネットにマップする FlexConnect AP 間をローミングするクライアントは、ローミング先のネットワークに適したアドレスとなるように、自身の IP アドレスを更新します。

無線リソース管理

接続モードの間、すべての無線リソース管理（RRM）機能は、基本的に使用可能です。ただし、一般的な FlexConnect 展開は少数の AP で構成されているため、ブランチ ロケーションで RRM 機能が動作しない場合があります。たとえば、伝送パワー コントロール（TPC）を行うには、最低 4 ヵ所の FlexConnect AP がお互いに近接している必要があります。TPC なしでは、カバレッジ ホール保護などの機能が使用できません。

ロケーション サービス

FlexConnect 展開は一般的に、所定のロケーションで少数の AP のみで構成されます。シスコでは、高レベルのロケーション確度を達成するため、AP の数と配置に関する厳格なガイドラインを用意しています。このため、FlexConnect 展開からロケーション情報を取得することも可能ですが、リモート ロケーション展開で確度のレベルは大きく異なる可能性があります。

QoS の考慮事項

中央でスイッチングされる WLAN では、FlexConnect AP は標準の AP と同様に QoS を処理します。ローカルにスイッチングされる WLAN は、異なる方法で QoS を実装します。

Wi-Fi MultiMedia（WMM）トラフィックを扱う、ローカルにスイッチングされる WLAN の場合、AP はアップストリーム トラフィックに対する dot1q VLAN タグ内の dot1p 値をマーク付けします。これはタグ付き VLAN でのみ行われ、ネイティブ VLAN では行われません。

ダウンストリーム トラフィックの場合、FlexConnect はローカルにスイッチングされるイーサネットから受信する dot1p タグを使用し、RF リンクを介して所定のユーザ宛てに送信されるフレームに関連付けられている WMM 値をキューに入れ、マーク付けします。

アップストリームとダウンストリームの両方のパケットで WLAN QoS プロファイルが適用されます。ダウンストリームでは、デフォルトの WLAN 値より高い 802.1p 値を受信した場合、デフォルトの WLAN 値が使用されます。アップストリームでは、クライアントがデフォルトの WLAN 値よりも高い WMM 値を送信すると、デフォルトの WLAN 値が使用されます。WMM 以外のトラフィックでは、AP からのクライアント フレームに CoS マーキングは含まれません。

詳細については、第 5 章「Cisco Unified Wireless QoS、AVC および ATF」を参照してください。

（注）　シスコでは、DSCP 設定に基づいてトラフィックが正しく処理されるように、適切なキューイング/ポリシング メカニズムを WAN 全体で実装することを強く推奨します。輻輳が原因となり、FlexConnect AP が接続モードとスタンドアロン モードとの切り替えを繰り返してしまう事態を防止するため、CAPWAP 制御トラフィック用の適切なプライオリティ キューを予約する必要があります。

FlexConnect ソリューション

FlexConnect ソリューションは、以下を実現します。

- トラフィックの中央集中型制御および管理
- 各ブランチ オフィスでのクライアント データ トラフィックの分散
- トラフィック フローを最も効率的な方法で確実に宛先に送信

アクセス ポイントの制御トラフィックを中央で集中管理する利点

AP 制御トラフィックを中央で集中管理する利点は、次のとおりです。

- モニタリングとトラブルシューティングの一括管理
- 管理の容易性
- データセンター リソースへのセキュアでシームレスなモバイル アクセス

- ブランチの占有面積の削減
- 運用コスト節約の向上

クライアント データ トラフィックを分散する利点

クライアント データ トラフィックを分散する利点は、次のとおりです。

- WAN リンクが完全に停止した場合や、コントローラが使用不能になった場合でも、運用上のダウンタイムが生じない（サバイバビリティ）
- WAN リンクで障害が発生した場合の、ブランチ内のモビリティの回復力。
- ブランチの拡張性の向上最大 100 ヵ所の AP および 250,000 平方フィート（AP あたり 5000 平方フィート）まで拡張可能なブランチの規模をサポート

中央クライアント データ トラフィック

Cisco FlexConnect ソリューションは、中央クライアント データ トラフィックもサポートしますが、ゲスト データ トラフィックのみに制限されます。表 7-1 と 表 7-2 は、データ トラフィックが中央のデータセンターでもスイッチングされるゲスト クライアント以外にのみ適用される、WLAN セキュリティ タイプの制限の概要を示します。

表 7-1　中央でスイッチングされるゲスト ユーザ以外のレイヤ 2 セキュリティのサポート

WLAN レイヤ 2 セキュリティ	タイプ	結果
なし	該当なし	許可
WPA + WPA2	802.1x	許可
	CCKM	許可
	802.1x + CCKM	許可
	PSK	許可
802.1x	WEP	許可
Static WEP	WEP	許可
WEP + 802.1x	WEP	許可
CKIP	—	許可

（注） これらの認証の制限は、データ トラフィックが各ブランチに分散されるクライアントには適用されません。

表 7-2　中央およびローカルにスイッチングされるユーザのレイヤ 3 セキュリティのサポート

WLAN レイヤ 3 セキュリティ	タイプ	結果
Web Authentication	内部	許可
	外部	許可
	カスタマイズ	許可
Web パススルー	内部	許可
	外部	許可
	カスタマイズ	許可
Conditional Web リダイレクト	外部	許可
スプラッシュ ページ リダイレクト	External	許可

主要な設計要件

FlexConnect AP はブランチ サイトに展開され、WAN リンクを介してデータセンターから管理されます。AP あたりの最小帯域幅制限を 24 kbps に維持し、ラウンドトリップ遅延を 300 ミリ秒以下に抑えることを強く推奨します（表 7-3 を参照）。

最大伝送ユニット（MTU）は、500 バイト以上にする必要があります。

表 7-3　帯域幅の最小値

展開タイプ	WAN 帯域幅（最小）	WAN RTT 遅延（最大）	ブランチあたり AP 数（最大）	ブランチあたりクライアント数（最大）
データ	64 kbps	300 ms	5	25
データ	640 kbps	300 ms	50	1000
データ	1.44 Mbps	1 秒	50	1000
データ + 音声	128 kbps	100 ms	5	25
データ + 音声	1.44 Mbps	100 ms	50	1000
データ + Flex AVC	75 Kbps	300 ms	5	25

主要な設計要件は次のとおりです。

- 最大 100 ヵ所の AP および 250,000 平方フィート（AP あたり 5000 平方フィート）まで拡張できるブランチの規模をサポート
- 一元的な管理およびトラブルシューティング
- 運用上のダウンタイムなし
- クライアント ベースのトラフィック セグメンテーション
- コーポレート リソースへのシームレスで、セキュアなワイヤレス接続
- PCI 準拠
- ゲストのサポート

FlexConnect グループ

各ブランチ サイトのすべての FlexConnect AP により、1 つの FlexConnect グループが構成されるため、FlexConnect グループの使用によって各ブランチ サイトの構成が簡素化します。

(注)　FlexConnect グループは、AP グループに類似するものではありません。

FlexConnect グループは主に、次のような課題を解決するよう設計されています。

- コントローラで障害が発生した場合、ワイヤレス クライアントはどのようにして 802.1X 認証を行い、データセンターのサービスにアクセスすればいいですか。
- ブランチとデータセンターの間の WAN リンクで障害が発生した場合、ワイヤレス クライアントはどのようにして 802.1X 認証を行えばいいですか。
- WAN で障害が発生した場合、ブランチのモビリティに影響がありますか。
- FlexConnect ソリューションでは、ブランチの運用上のダウンタイムがなくなるのですか。

スタンドアロン モードの FlexConnect AP がバックアップ RADIUS サーバに対して完全な 802.1X 認証を実行できるように、コントローラを設定することができます。

(注)　バックアップ RADIUS アカウンティングはサポートされません。

ブランチの復元力を高めるために、管理者はプライマリ バックアップ RADIUS サーバ、またはプライマリ/セカンダリ バックアップ RADIUS サーバの両方を設定できます。これらのサーバは FlexConnect AP がコントローラに接続されていない場合にのみ使用されます。

デフォルトの FlexConnect グループ数

リリース 8.4 では、コントローラに Default Flex Connect Group オプションが追加されました。8.4 より前のリリースでは、FC 設定は FC グループを通じてのみ可能であり、グループ内でサポートされる AP 数に制限がありました。AP 数が膨大で、一部の設定が類似している小売業での導入では、アクセス ポイントのプロビジョニングのために多数の FC グループを作成するのは面倒な作業です。解決策として、default-apgroup と類似する default-flex-group を使用できます。管理者が設定した FC グループに含まれない FC モードである AP がコントローラに接続すると、AP は default-flexgroup に属することになり、このグループから設定を取得します。

コントローラが起動すると、「default-flexgroup」が作成されて保存されます。このグループは手動で削除または追加することはできません。同様に、default-flexgroup に対して、アクセス ポイントを手動で追加または削除することもできません。このグループには、いくつかのパラメータについてグループ作成時のデフォルト設定があり（管理者が設定する他のグループと同様）、グループに属する AP の最大数に制限はありません。設定の変更は、グループに属するすべての AP に伝播されます。グループの設定はリセットしても保持されます。

管理者が設定したグループが削除されるか、AP がグループから手動で削除されると、その AP は default-flexgroup に属し、このグループから設定を継承します。カスタマイズされたグループに AP が追加された場合は、default-flexgroup 設定が削除され、新しい設定が AP にプッシュされます。

次の機能はサポートされていません。

- 効率的なイメージ アップグレード?
- PMK キャッシュ分散?
- 高速ローミング

次の機能はサポートされています:?

- VLAN サポート（ネイティブ VLAN、WLAN-VLAN マッピング）
- VLAN ACL マッピング?
- Web 認証、Web ポリシー、ローカル スプリット マッピング?
- ローカル認証ユーザ?
- RADIUS 認証?
- 中央 DHCP または NAT-PAT?
- フレックス AVC
- VLAN 名 ID マッピング?
- マルチキャスト オーバーライド

その他の設定の詳細については、『Controller Configuration Guide（コントローラ設定ガイド）』を参照してください。

FlexConnect グループの設定

FlexConnect が接続モードまたはスタンドアロン モードのときに、ローカル拡張認証プロトコル（LEAP）を使用したローカル認証をサポートするように FlexConnect グループを設定するには、次の手順を実行します。

ステップ 1　[Wireless] > [FlexConnect Groups] の下の [New] をクリックします。

ステップ 2　グループ名を Store 1 として割り当てます。

ステップ 3　グループ名を設定したら、[Apply] をクリックします。

ステップ 4　新しく作成したグループ名 Store 1 をクリックします。

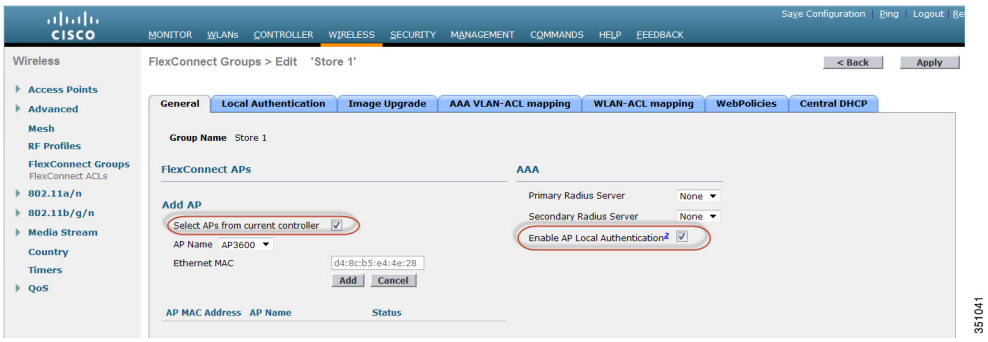
ステップ 5　[Add AP] をクリックします。

ステップ 6　AP がスタンドアロン モードのときにローカル認証を有効にするには、[Enable AP Local Authentication] チェックボックスをオンにします。

ステップ 7　[AP Name] ドロップダウン メニューを有効にするには、[Select APs from current controller] チェックボックスをオンにします。

ステップ 8　この FlexConnect グループに含める必要がある AP を [AP Name] ドロップダウン メニューから選択します。

ステップ 9　[Add] をクリックします。



ステップ 10　ステップ 7 とステップ 8 を繰り返し、この FlexConnect グループ Store 1 に必要なすべての AP を追加します。

(注)　AP グループと FlexConnect グループ間の比率を 1 対 1 に維持することにより、ネットワーク管理を簡略化できます。

ステップ 11　[Local Authentication] > [Protocols] タブに移動し、[Enable LEAP Authentication] チェックボックスをオンにします。

ステップ 12　[Apply] をクリックします。

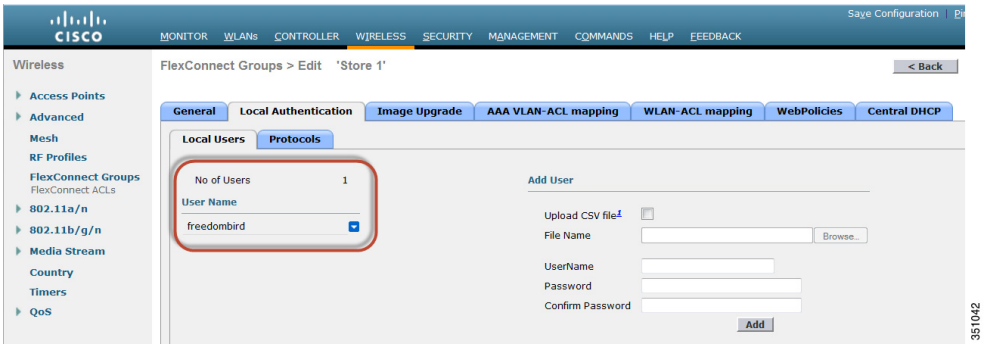
(注)　バックアップ コントローラがある場合は、双方の FlexConnect グループが同一であり、FlexConnect グループごとに AP の MAC アドレス エントリが含まれていることを確認します。

ステップ 13　[Local Authentication] > [Local Users] タブに移動します。

ステップ 14　AP 上にある LEAP サーバ内にユーザ エントリを作成するには、[UserName]、[Password]、および [Confirm Password] フィールドを設定し、[Add] をクリックします。

ステップ 15　ステップ 13 を繰り返し、必要なローカル ユーザ名をすべて追加します。100 人を超えるユーザを設定または追加することはできません。

ステップ 16　すべてのローカル ユーザ情報の入力が完了したら、[Apply] をクリックします。ユーザ数が検証されます。

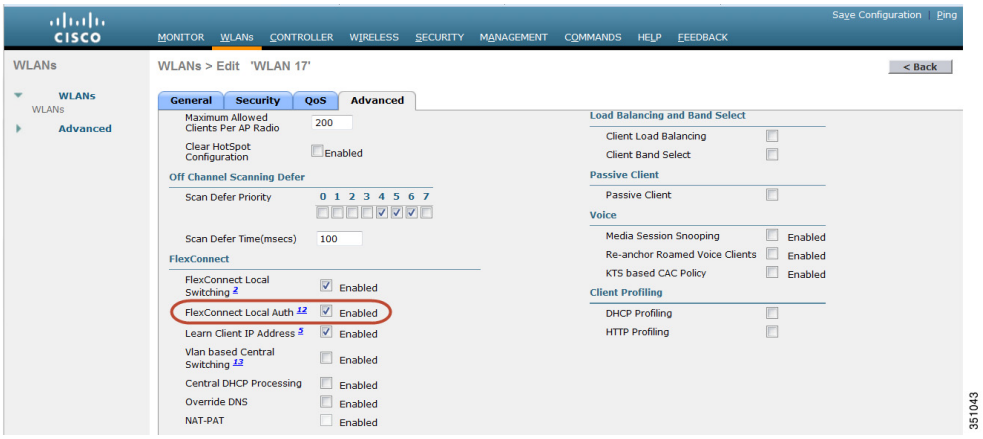


ステップ 17　上部のペインで [WLANs] をクリックします。

ステップ 18　AP グループの作成時に作成された [WLAN ID] 番号をクリックします。この例では WLAN 17 です。

ステップ 19　[WLAN] > [Edit for WLAN ID 17] の下の [Advanced] をクリックします。

ステップ 20　接続モードでローカル認証を有効にするには、[FlexConnect Local Auth] チェックボックスをオンにします。



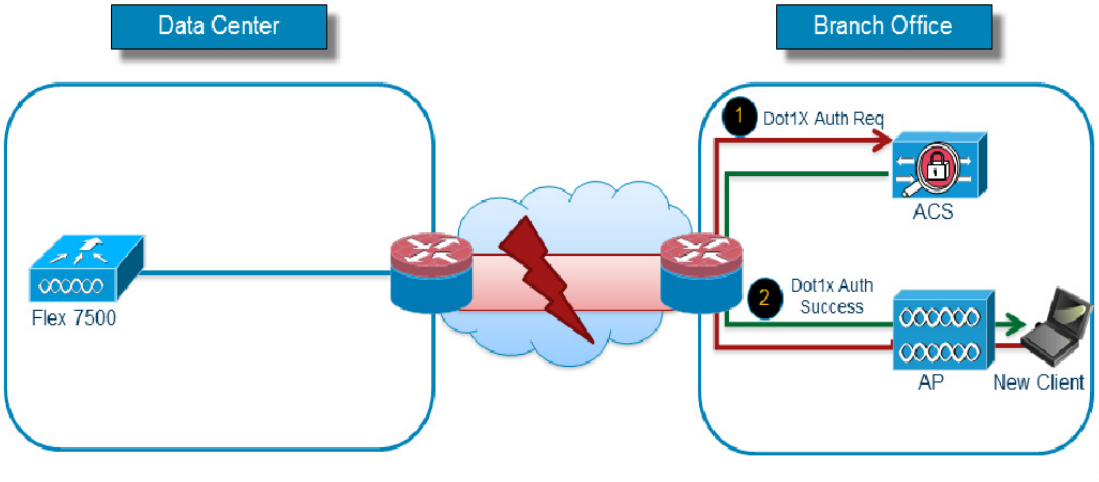
(注)　ローカル認証は、ローカル スイッチングを使用する FlexConnect のみでサポートされます。WLAN の下でローカル認証を有効化する前に、必ず FlexConnect グループを作成してください。

ローカル認証

図 7-8 に示すように、FlexConnect ブランチ AP がコントローラとの接続を失った場合でも、クライアントは引き続き 802.1X 認証を実行できます。RADIUS/ACS サーバにブランチ サイトから到達可能な限り、ワイヤレス クライアントは、引き続き認証とワイヤレス サービスへのアクセスを行います。

つまり、RADIUS/ACS がブランチ内部にあれば、クライアントは WAN が停止している間でも、認証とワイヤレス サービスへのアクセスを行います。

図 7-8　ローカル認証:AP オーセンティケータ



- WAN の障害、WLC の障害、および RADIUS サーバの障害を視野に入れ、ブランチの復元力を強化するためにローカル バックアップ RADIUS サーバを設定します。
- この機能は、セントラル サイトとの WAN 遅延が大きいリモート オフィスでも使用されます。
- プライマリ バックアップ RADIUS サーバを設定することも、プライマリとセカンダリの両方のバックアップ RADIUS サーバを設定することもできます。スタンドアロン モードの FlexConnect AP は、バックアップ RADIUS サーバに対して完全な 802.1X 認証を実行するように設定できます。
- これらのサーバは、FlexConnect AP がコントローラに接続されていない場合か、または WLAN がローカル認証用に設定されている場合に使用されます。
- RADIUS/ACS がブランチ内部にある場合、クライアントは WAN が停止している間でも、認証とワイヤレス サービスへのアクセスを行います。

(注)　ローカル バックアップ RADIUS サーバを設定する場合は、次の制限事項に注意してください。ローカル バックアップ RADIUS サーバをブランチで使用する場合は、オーセンティケータとして機能するすべての AP の IP アドレスを、この RADIUS サーバに追加する必要があります。

(注)　ローカル認証機能は、FlexConnect バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループにバックアップ RADIUS サーバ機能とローカル認証機能の両方を設定した場合、FlexConnect AP はまず、プライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。次に、セカンダリ バックアップ RADIUS サーバによる認証を試行し(プライマリに到達できない場合)、最後に FlexConnect AP 自体のローカルな EAP サーバによる認証を試行します(プライマリとセカンダリの両方に到達できない場合)。

ローカル EAP

スタンドアロン モードまたは接続モードの FlexConnect AP が、最大 100 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるように、コントローラを設定できます。特定の FlexConnect グループがコントローラに参加すると、コントローラはユーザ名およびパスワードの静的リストを、この FlexConnect グループ内の個々の FlexConnect AP に送信します。グループ内の各 AP は、自身にアソシエートされたクライアントのみを認証します。

この機能が適しているのは、カスタマーがスタンドアロン AP ネットワークから軽量な FlexConnect AP ネットワークに移行するときに、大きなユーザ データベースを保持したくない場合や、スタンドアロン AP で利用可能な RADIUS サーバ機能を置き換える、新たなハードウェア デバイスを追加したくない場合です。

PEAP、EAP-TLS 認証のサポート

FlexConnect AP は LEAP および EAP-FAST クライアント認証用の RADIUS サーバとして設定できます。スタンドアロン モードであり、WLAN 上でローカル認証機能が有効にされている場合は、FlexConnect AP はローカル RADIUS を使用して、AP 自身の dot1x（802.1X）認証を行います。リリース 7.5 のコントローラでは、PEAP、EAP-TLS の EAP 方式もサポートされます。

CCKM/OKC 高速ローミング

Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミングで FlexConnect AP を使用する場合には、FlexConnect グループが必要となります。高速ローミングは、ワイヤレス クライアントを別の AP にローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスター キーの派生キーをキャッシュすることにより実現します。

この機能により、クライアントをある AP から別の AP へローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。

しかし、たとえば 300 の AP を持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対する CCKM/OKC キャッシュを送信することは現実的ではありません。限定した数の AP から成る FlexConnect グループを作成すれば（たとえば、1 つのリモート オフィス内の 4 つの AP のグループを作成）、クライアントはその 4 つの AP 間でのみローミングします。CCKM/OKC キャッシュがその 4 つの AP 間で配布されるのは、クライアントがそのいずれかにアソシエートするときだけとなります。

この機能とバックアップ RADIUS およびローカル認証（ローカル EAP）により、ブランチ サイトの運用上のダウンタイムがなくなります。

FlexConnect グループは、FlexConnect AP が接続モードまたはスタンド アロンモードであり、クライアントに CCKM/OKC 高速ローミングが必要な場合に使用します。

この機能により、クライアントが AP から別の AP へローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。

FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。

（注）　CCKM/OKC 高速ローミングは FlexConnect AP でのみサポートされます。

FlexConnect VLAN オーバーライド

現在の FlexConnect アーキテクチャでは、WLAN から VLAN への厳密なマッピングが行われます。このため、FlexConnect AP 上で特定の WLAN にアソシエートされたクライアントは、この WLAN にマッピングされる VLAN に従う必要があります。この方式は、異なる VLAN ベースのポリシーを継承するために、クライアントを異なる SSID にアソシエートする必要があるので、さまざまな制約があります。

リリース 7.2 以降では、ローカル スイッチングが設定された個々の WLAN に対する、VLAN の AAA オーバーライドがサポートされています。AP には、動的に VLAN を割り当てるために、個々の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、または FlexConnect グループの ACL-VLAN マッピングを使用した設定に基づいて事前に作成された、VLAN 用のインターフェイスがあります。AP でサブインターフェイスを事前作成するために、WLC が使用されます。

FlexConnect VLAN オーバーライドの要約

- AAA VLAN オーバーライドは、中央およびローカル認証モードでローカル スイッチングが設定された WLAN に対し、リリース 7.2 からサポートされています。
- AAA オーバーライドは、ローカル スイッチングが設定された WLAN 上で有効にする必要があります。
- FlexConnect AP には、動的な VLAN 割り当て用に、WLC から VLAN が事前に作成されている必要があります。
- AAA オーバーライドから返された VLAN が AP クライアント上にない場合、IP は AP のデフォルト VLAN インターフェイスから取得されます。

FlexConnect VLAN に基づく中央スイッチング

リリース 7.3 以降では、FlexConnect AP からのトラフィックは、FlexConnect AP 上に VLAN が存在するかどうかに応じて、中央またはローカルでスイッチングされます。

コントローラ ソフトウェア リリース 7.2 では、ローカルにスイッチングされる WLAN に対する VLAN の AAA オーバーライド（動的な VLAN 割り当て）により、AAA サーバから提供される VLAN 上にワイヤレス クライアントが配置されます。AAA サーバから提供された VLAN が AP に存在しない場合、クライアントはその AP 上で WLAN にマッピングされた VLAN に配置され、トラフィックはこの VLAN 上でローカルにスイッチングされます。さらに、7.3 よりも前のリリースでは、FlexConnect AP からの特定の WLAN のトラフィックは、WLAN の設定に応じて中央またはローカルでスイッチングされます。

FlexConnect VLAN 中央スイッチングの要約

FlexConnect AP が接続モードの場合に、ローカル スイッチングが設定された WLAN 上のトラフィック フローは、次のようになります。

- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在しない場合、トラフィックは中央でスイッチングされます。この VLAN が WLC 上に存在する場合は、AAA サーバから返されたこの VLAN とインターフェイスがクライアントに割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在しない場合、トラフィックは中央でスイッチングされます。その VLAN が WLC にも存在しない場合、クライアントには WLC 上で WLAN にマッピングされた VLAN とインターフェイスが割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在する場合、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

FlexConnect AP がスタンドアロン モードの場合に、ローカル スイッチングが設定された WLAN 上のトラフィック フローは、次のようになります。

- AAA サーバによって返された VLAN が FlexConnect AP データベースに存在しない場合、クライアントはデフォルト VLAN（つまり、FlexConnect AP 上で WLAN にマッピングされた VLAN）に配置されます。AP が接続モードに戻ると、このクライアントは認証を解除され、トラフィックが中央でスイッチングされます。
- AAA サーバによって返された VLAN が FlexConnect AP データベースに存在する場合、クライアントは返された VLAN に配置され、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

VLAN 名のオーバーライド

VLAN 名のオーバーライド機能は、中央の 1 つの RADIUS サーバによって複数のブランチを認証する構成で役立ちます。ブランチの数が数百規模に及ぶ場合、全サイトで VLAN の ID を標準化することは非常に困難です。この場合、ブランチ ロケーションごとに異なる VLAN ID にローカルにマッピングされる、一意の VLAN 名を提供する設定が必要となります。

このように、サイトごとに異なる VLAN ID を使用する設計では、レイヤ 2 ブロードキャスト ドメインあたりのクライアント数を制限できるため、サイジングと拡大縮小の観点からも有益です。

FlexConnect VLAN 名オーバーライドの要約

- VLAN 名オーバーライド機能は、ローカル スイッチング WLAN での中央およびローカル認証の両方に対応します。
- AAA サーバから複数の VLAN 属性が返される場合は、VLAN 名属性が優先されます。
- Aire-Interface-Name 属性と Tunnel-Private-Group-ID 属性の両方が返される場合は、Tunnel-Private-Group-ID 属性のほうが優先されます。

- AAA サーバから不明の VLAN 名属性が返された場合、クライアントには、AP 上に存在する WLAN-VLAN ID マッピングがデフォルトで適用されます。
- この機能は、スタンドアロン モードでもサポートされます。

FlexConnect ACL

FlexConnect 上での ACL の導入に伴い、AP からローカルにスイッチングされるデータ トラフィックの保護と整合性のために、FlexConnect AP でのアクセス制御の必要性を満たすメカニズムが用意されています。FlexConnect ACL を WLC 上に作成し、VLAN-ACL マッピングを使用して、この ACL に FlexConnect AP 上の VLAN または FlexConnect グループ上の VLAN（AAA オーバーライド VLAN 用）を設定する必要があります。これらの ACL は AP にプッシュされます。

FlexConnect ACL の要約

- コントローラ上に FlexConnect ACL を作成します。
- この ACL を、AP レベルでの VLAN ACL マッピングに基づき、FlexConnect AP 上に存在する VLAN に適用します。
- VLAN-ACL マッピングに基づき、FlexConnect グループに存在する VLAN にも適用できます（一般に AAA オーバーライドされた VLAN に対して行います）。
- VLAN に対して ACL を適用する際に、適用する方向として、*ingress*、*egress*、または *ingress and egress* を選択します。

FlexConnect ACL の制限事項

- 1 つの WLC には、最大 512 個の FlexConnect ACL を設定できます。
- 個々の ACL には 64 個のルールを設定できます。
- FlexConnect グループまたは FlexConnect AP あたり最大 32 個の ACL をマッピングできます。
- FlexConnect AP 上には、一度に最大 16 の VLAN と 32 個の ACL を設定できます。

クライアント ACL サポート

リリース 7.5 以前では、VLAN で FlexConnect ACL がサポートされます。また、VLAN の AAA オーバーライドもサポートされます。クライアントに対して VLAN の AAA オーバーライドが行われた場合、このクライアントはオーバーライドされた VLAN 上に配置され、この VLAN の ACL が適用されます。ローカルにスイッチされるクライアントに対し、AAA サーバから ACL が送られてきた場合は、この ACL は無視されます。リリース7.5ではこの制限事項が解決され、ローカルにスイッチされる WLAN に対し、クライアント ベースの ACL がサポートされます。

FlexConnect スプリット トンネリング

スプリット トンネリングにより、クライアントによって送信されたトラフィックを、FlexConnect ACL を使用し、パケットの内容に基づいて分類するメカニズムが導入されました。一致するパケットは FlexConnect AP からローカルにスイッチングされ、それ以外のパケットは CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング機能には、企業の SSID 上のクライアントがローカル ネットワーク上のデバイス（プリンタ、リモート LAN ポート上の有線マシン、またはパーソナル SSID 上のワイヤレス デバイス）と直接通信でき、CAPWAP を介してパケットを送信することで WAN 帯域幅を消費することがないという、OEAP 構成に対するさらなるメリットがあります。

適切なルールを規定した FlexConnect ACL を作成することで、ローカル サイトまたはネットワークに存在するすべてのデバイスを許可できます。企業の SSID 上のワイヤレス クライアントからのパケットが、OEAP 上で設定されている FlexConnect ACL のルールに一致した場合、そのトラフィックはローカルにスイッチングされ、それ以外のトラフィック（つまり暗黙的に拒否されたトラフィック）は、CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング ソリューションでは、セントラル サイトのクライアントにアソシエートされているサブネットまたは VLAN が、ローカル サイトには存在しないことを前提としています（つまり、セントラル サイトにあるサブネットから IP アドレスを受け取るクライアントのトラフィックは、ローカルにスイッチングできません）。

スプリット トンネリングは、WAN 帯域幅の消費を軽減するために、ローカル サイトに属するサブネットに対してトラフィックをローカルにスイッチングするように設計された機能です。FlexConnect ACL ルールに一致するトラフィックはローカルにスイッチングされます。NAT 操作の実行により、クライアントの送信元 IP アドレスは、ローカル サイトまたはネットワークでルーティング可能な FlexConnect AP のインターフェイス IP アドレスに変更されます。

スプリット トンネルの要約

- スプリット トンネリング機能は、FlexConnect AP のみによってアドバタイズされる、中央でのスイッチングが設定された WLAN 上でサポートされます。
- スプリット トンネリングを設定した WLAN 上では、必要な DHCP を有効化する必要があります。
- スプリット トンネリングの設定は、FlexConnect AP ごと、または FlexConnect グループ内のすべての FlexConnect AP に対して、中央スイッチングが設定された WLAN ごとに適用されます。

スプリット トンネリングの制限事項

- FlexConnect ACL ルールは、同じサブネットを送信元および宛先とする permit/deny 文を使用して設定できません。
- スプリット トンネリングが設定された、中央でスイッチングされる WLAN 上のトラフィックをローカルにスイッチングできるのは、ワイヤレス クライアントがローカル サイト上にあるホスト宛のトラフィックを送信した場合のみです。トラフィックが、ローカル サイト上のクライアントまたはホストにより、上記のとおり設定された WLAN 上のワイヤレス クライアントに送信された場合は、宛先に到達できません。

- マルチキャストまたはブロードキャスト トラフィックについては、スプリット トンネリングはサポートされていません。マルチキャストまたはブロードキャスト トラフィックは、FlexConnect ACL に一致しても中央でスイッチングされます。
- スプリット トンネル機能は、外部アンカー ローミング シナリオではサポートされていません。

耐障害性

FlexConnect の耐障害性機能により、FlexConnect AP で次の状態が生じた場合でも、ブランチ クライアントに対するワイヤレス アクセスとサービスが可能になります。

- プライマリ コントローラへの接続を失ったとき。
- セカンダリ コントローラに切り替わるとき。
- プライマリ コントローラとの接続を再確立するとき。

FlexConnect の耐障害性とローカル EAP とを組み合わせることで、ネットワーク停止時のゼロ ブランチ ダウンタイムを実現できます。この機能はデフォルトで有効であり、無効にすることはできません。つまり、コントローラまたは AP での設定は不要です。ただし、耐障害性が円滑に機能し、適用可能であるためには、次の条件を満たす必要があります。

- WLAN の順序と設定は、プライマリおよびバックアップ コントローラで同じであることが必要です。
- VLAN マッピングは、プライマリおよびバックアップ コントローラで同じであることが必要です。
- モビリティ ドメイン名は、プライマリおよびバックアップ コントローラで同じであることが必要です。
- プライマリおよびバックアップ コントローラとして FlexConnect 7500 を使用する必要があります。

耐障害性の要約

- コントローラの設定を変更しない限り、FlexConnect AP が同じコントローラに再接続する場合、クライアントが切断されることはありません。
- 設定に変更がなく、バックアップ コントローラがプライマリ コントローラと同じである限り、FlexConnect AP がバックアップ コントローラに接続する場合、クライアントが切断されることはありません。
- コントローラの設定に変更がない限り、FlexConnect AP がプライマリ コントローラに再接続する場合、その無線はリセットされません。

耐障害性の制限事項

- ローカル スイッチングによる、中央またはローカルの認証を使用する FlexConnect のみでサポートされます。
- 中央で認証されるクライアントは、FlexConnect AP がスタンドアロン モードから接続モードに切り替わる前にクライアント セッション タイマーが切れた場合、完全な再認証が必要となります。
- プライマリおよびバックアップ コントローラは、同じモビリティ ドメインに属している必要があります。

ピアツーピア ブロッキング

ピアツーピア(P2P)ブロッキングは、ローカル スイッチング WLAN にアソシエートされたクライアントに対してサポートされます。WLAN ごとのピアツーピア設定は、コントローラによって FlexConnect AP にプッシュされます。P2P ブロッキングでは、WLAN に対して次の 3 つのいずれかの動作を設定できます。

- 無効化:P2P ブロッキングを無効にし、同じサブネット内のクライアント宛のトラフィックをコントローラ内でローカルにブリッジします。これはデフォルト値です。
- ドロップ:コントローラは同じサブネット内のクライアント宛のパケットを破棄します。
- アップストリーム転送:パケットはアップストリーム VLAN に転送されます。コントローラ上のデバイスは、パケットに関して実行すべきアクションを決定します。

P2P の要約

- P2P ブロッキングは、WLAN ごとに設定します。
- WLAN ごとの P2P ブロッキングの設定は、WLC によって FlexConnect AP にプッシュされます。
- WLAN 上で P2P ブロッキング アクションをドロップまたはアップストリーム転送として設定すると、FlexConnect AP では P2P ブロッキングが有効化されたとみなされます。

P2P の制限事項

- FlexConnect ソリューションでは、特定の FlexConnect AP または AP のサブセットのみに P2P ブロッキング設定を適用することはできません
- これは、SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチング クライアントのための統一ソリューションは、P2P アップストリーム転送をサポートしています。しかし、これは FlexConnect ソリューションでサポートされません。これは、P2P ドロップとして扱われ、クライアント パケットは、次のネットワーク ノードに転送されずにドロップされます。
- 中央スイッチング クライアント用の統一ソリューションは、異なる AP にアソシエートされたクライアントに対する P2P ブロッキングをサポートしています。ただし、このソリューションでは、同一の AP に接続するクライアントだけがターゲットとなります。この制限の回避策として、FlexConnect ACL を使用できます。

ローカル スイッチング WLAN のための FlexConnect WGB/uWGB サポート

リリース 7.3 から、シスコのワーク グループ ブリッジとユニバーサル ワーク グループ ブリッジ(WGB/uWGB)、および WGB の背後にある有線またはワイヤレス クライアントがサポートされ、ローカル スイッチングが設定された WLAN 上の通常のクライアントとして動作します。

アソシエーションの後、WGB は各有線またはワイヤレス クライアントに IAPP メッセージを送信し、これに対して FlexConnect AP は次のように動作します。

- FlexConnect AP が接続モードの場合、すべての IAPP メッセージをコントローラに転送し、コントローラはローカル モード AP と同様に IAPP メッセージを処理します。有線またはワイヤレス クライアント宛のトラフィックは、FlexConnect AP からローカルにスイッチングされます。
- スタンドアロン モードの AP は、IAPP メッセージを処理します。WGB 上の有線またはワイヤレス クライアントは、登録と登録解除を行うことができる必要があります。FlexConnect AP は接続モードに移行するときに、有線クライアントの情報をコントローラに送信します。FlexConnect AP がスタンドアロン モードから接続モードに移行するとき、WGB は登録メッセージを 3 回送信します。

  有線またはワイヤレス クライアントは WGB の設定を継承します。つまり、AAA 認証、AAA オーバーライド、FlexConnect ACL などの個別の設定は、WGB の背後にあるクライアントについては不要です。

FlexConnect WGB/uWGB の要約

- FlexConnect AP 上で WGB をサポートするために、WLC 上で特別な設定は不要です。
- 耐障害性は、WGB および WGB の背後にあるクライアントに対してサポートされています。
- WGB がサポートされている IOS AP は、1240、1130、1140、1260、1250 です。

FlexConnect WGB/uWGB の制限事項

- WGB の背後にある有線クライアントは、常に WGN 自体と同じ VLAN にあります。ローカル スイッチングが設定された WLAN の FlexConnect AP では、WGB 背後のクライアントに対する複数 VLAN はサポートされません。
- ローカル スイッチングが設定された WLAN 上の FlexConnect AP にアソシエーションされている場合、WGB の背後では、最大 20 台のクライアント（有線またはワイヤレス）がサポートされています。
- ローカル スイッチングが設定された WLAN にアソシエーションされている WGB の背後にあるクライアントについては、WebAuth はサポートされません。

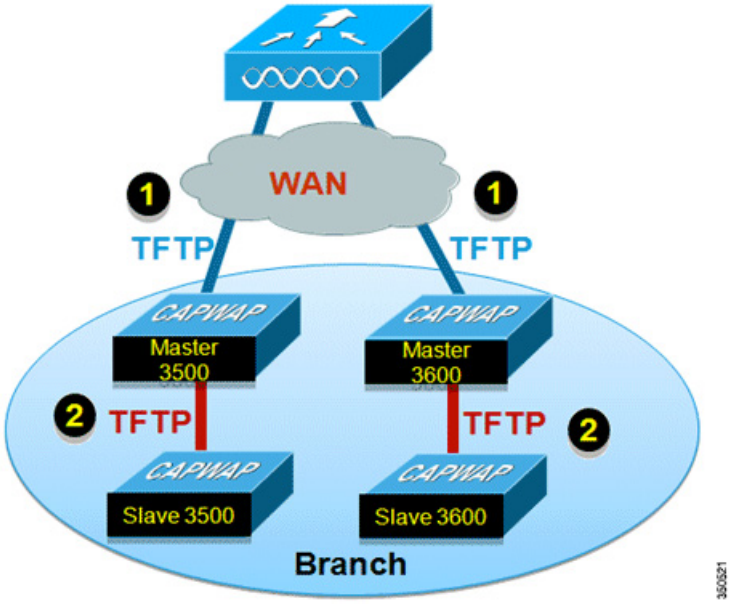
FlexConnect AP イメージのスマート アップグレード

イメージのプレダウンロード機能は、ダウンタイムをある程度削減する効果があります。しかし、すべての FlexConnect AP は WAN リンク経由でそれぞれの AP イメージをプレダウンロードしなければならないため、大幅な遅延が発生します。

効率的な AP イメージ アップグレードでは、個々の FlexConnect AP のダウンタイムが削減されます。基本的な原理は、各 AP モデルにつき、それぞれ 1 つの AP のみがコントローラからイメージをダウンロードし、マスター（サーバ）として機能します。同モデルのその他の AP はスレーブ（クライアント）となり、マスターから AP イメージをプレダウンロードします。

サーバからクライアントへの AP イメージの配布はローカル ネットワーク上で行われるため、WAN リンクで遅延が発生しません。この結果、プロセスの実行時間が短縮されます。

図 7-9　　AP イメージのスマート アップグレード



AP イメージのスマート アップグレードの要約

- FlexConnect グループごとに、各 AP モデルのマスターおよびスレーブ AP が選出されます。
- マスターは WLC からイメージをダウンロードします。
- スレーブは、マスター AP からイメージをダウンロードします。
- ダウンタイムが削減され、WAN帯域幅を節約できます。

FlexConnect ローカル スイッチングの VideoStream

リリース 8.0 では、ブランチ オフィス環境用に、ローカル スイッチングによる VideoStream 機能が導入されました。

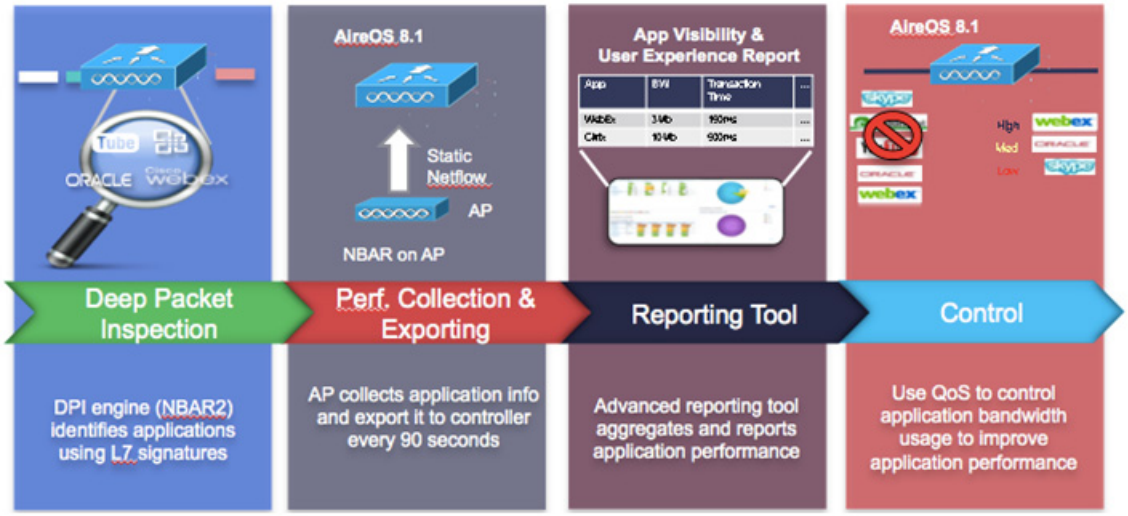
この機能により、エンタープライズ環境で現在実現されている機能と同様に、ワイヤレス アーキテクチャでも、ブランチ間のマルチキャスト ビデオ ストリーミングの展開が可能となります。

この機能は、ブランチ ネットワーク内でビデオ ストリームとクライアントの規模を拡大する場合に、ビデオ配信の質が低下するという欠点を補います。VideoStream は、ワイヤレス クライアントに対するビデオ マルチキャストの信頼性を高め、ブランチ内のワイヤレス帯域幅の使用効率を向上させます。

FlexConnect の Application Visibility and Control

AVC は、ワイヤレス ネットワークでのアプリケーション対応制御を可能にし、管理性と生産性を向上させます。AVC は、ASR、ISR G2 および WLC プラットフォーム上ですでにサポートされています。FlexConnect AP に組み込まれている AVC のサポートは、さらに機能拡張され、エンドツーエンドのソリューションとなっています。ネットワーク内のアプリケーションは完全に可視化され、管理者はアプリケーションに対し、特定のアクションを実行できます。

図 7-10　FlexConnect の Application Visibility and Control



- FlexConnect AP 上で NBAR2 エンジンが実行されます。
- DPI エンジン（NBAR2）を使用して、アクセス ポイントでアプリケーションの分類が行われ、L7 シグニチャを使用してアプリケーションが識別されます。
- AP はアプリケーション情報を収集し、90 秒ごとにコントローラにエクスポートします。
- リアルタイム アプリケーションは、コントローラのユーザ インターフェイスでモニタされます。
- FlexConnect アクセス ポイントで分類されたアプリケーションでは、アクション、ドロップ、マーキング、またはレート制限を実行できます。

AVC の仕様および制限

- FlexConnect AP の AVC では、1000 種類以上のアプリケーションを分類し、アクションを実行できます。
- FlexConnect AP で稼働するプロトコル パックは、WLC 上で稼働するプロトコルパックとは異なります。
- AVC による GUI の統計情報は、デフォルトでは上位 10 のアプリケーションに対して表示されます。これを、上位 20 または 30 のアプリケーションに変更することもできます。
- FlexConnect グループ内のローミングがサポートされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドはサポートされません。

- マルチキャスト トラフィックは、AVC アプリケーションではサポートされません。
- リリース 8.1 では、FlexConnect AVC の NetFlow エクスポートはサポートされません。

展開に関する一般的な考慮事項

- いずれの WLC でも FlexConnect AP をサポートすることは可能ですが、ブランチ ロケーションの数、および展開される AP 合計数に応じて、FlexConnect 展開をサポートするための専用 WLC の使用を検討することは（管理上の観点から）有効です。
- FlexConnect AP は一般的に、メイン キャンパス内の AP と同じポリシーは共有しません。各ブランチ ロケーションは、基本的にそれ自体が RF およびモビリティ ドメインです。単一の WLC を複数の論理 RF およびモビリティ ドメインに分割することはできませんが、専用 WLC を使用することで、ブランチ固有の設定およびポリシーを論理的にキャンパスから切り離すことができます。
- 専用 FlexConnect WLC を展開する場合は、メイン キャンパスのものとは異なるモビリティおよび RF ネットワーク名を使用して設定する必要があります。専用 WLC に参加するすべての FlexConnect AP は、その RF およびモビリティ ドメインのメンバーとなります。
- 自動 RF の観点から、WLC は十分な数の FlexConnect AP が所定のブランチ内に展開されていると想定し、各ブランチにアソシエートされている RF カバレッジを自動管理しようとします。
- 各 FlexConnect AP を独自のモビリティ ドメインに統合しても、利点も不都合もありません。これは、クライアント トラフィックがローカルにスイッチングされるためです。EoIP モビリティ トンネルは、クライアントが FlexConnect AP にローミングする（同じモビリティ ドメインの）WLC 間では実行されません。
- FlexConnect 展開に専用 WLC を使用する場合、ネットワークの可用性を確保するために、バックアップ WLC も展開する必要があります。標準の AP 展開と同様、指定の WLC とのアソシエーションが強制的に適用されるように、FlexConnect AP にも WLC 優先度を設定する必要があります。
- 分散ブランチ オフィスを展開する場合は、最小 WAN 帯域幅、最大 RTT、最小 MTU、フラグメンテーションなど、特定の構成要件を考慮する必要があります。
- 使用する AP モデルが FlexConnect をサポートしていることを確認します。AP モデル OEAP600 は、FlexConnect モードをサポートしていません。
- UDP ポート 5246 で CAPWAP 制御チャネルのトラフィックが優先されるように、QoS を設定します。
- 静的 IP アドレスまたは DHCP アドレスのいずれかを持つ FlexConnect AP を展開することができます。DHCP サーバがローカルで使用可能になっており、ブートアップ時に AP に IP アドレスを提供できる必要があります。
- FlexConnect は最大で 4 つの断片化されたパケット、または最低 500 バイトの最大伝送単位（MTU）WAN リンクをサポートします。
- ラウンドトリップ遅延は、AP とコントローラ間で 300 ミリ秒を超えないようにする必要があります。ラウンドトリップ遅延を 300 ミリ秒以下に抑えられない場合は、ローカル認証を実行するよう AP を設定します。
- FlexConnect には、堅牢な耐障害性手法が実装されています。AP とコントローラが同一の設定を有する場合、クライアントと FlexConnect AP 間の接続（再結合またはスタンバイ）はそのまま維持され、クライアントではシームレスな接続が行われます。

- FlexConnect AP のプライマリ コントローラとセカンダリ コントローラの設定が同一であることが必要です。そうでない場合、AP がその設定を失い、特定の機能（WLAN オーバーライド、VLAN、静的チャネル番号など）が期待どおりに動作しない場合があります。さらに、FlexConnect AP の SSID とそのインデックス番号が、両方のコントローラで同一であることを確認してください。
- クライアント接続は、AP がスタンドアロン モードから接続モードに移行するときに RUN 状態になっている、ローカルにスイッチングされたクライアントに対してのみ復元されます。AP がスタンドアロン モードから接続モードに移行すると、AP の無線もリセットされます。
- AP がコントローラへの接続を確立すると、セッション タイムアウトと再認証が行われます。
- セッション タイマーが切れると、クライアントのユーザ名、現在の（サポートされる）レート、リッスン インターバルの値はデフォルト値にリセットされます。クライアント接続が再確立されるときに、コントローラはクライアントの元の属性を復元しません。
- 複数の FlexConnect グループを 1 つのロケーションで定義できます。ロケーションごとの FlexConnect AP の展開数に制限はありません。
- FlexConnect モードでは、AP はユニキャスト形式でのみマルチキャスト パケットを受信できます。
- FlexConnect AP は、真のマルチキャストを除くすべての機能に対して、1 対 1 ネットワーク アドレス変換（NAT）設定とポート アドレス変換（PAT）をサポートします。ユニキャスト オプションを使用して設定されている場合、NAT の境界を越えるマルチキャストもサポートされます。FlexConnect AP は、中央でスイッチングされるすべての WLAN に対して真のマルチキャストが動作するようにしたい場合を除き、多対 1 の NAT/PAT 境界もサポートします。

（注） NAT と PAT は FlexConnect AP ではサポートされていますが、対応するコントローラではサポートされていません。シスコは、NAT/PAT 境界の背後にコントローラを置く構成はサポートしません。

- AP で、これらのセキュリティ タイプがローカルにアクセス可能である場合、VPN および PPTP は、ローカルにスイッチングされるトラフィックに対してサポートされます。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect ローカル スイッチング用に設定された WLAN ではサポートされません。
- ワーク グループ ブリッジおよびユニバーサル ワーク グループ ブリッジは、ローカルでスイッチングされるクライアントの FlexConnect AP でサポートされます。
- FlexConnect AP はクライアント ロード バランシングをサポートしません。
- FlexConnect は、IPv4 の動作と同様にトラフィックをローカル VLAN にブリッジすることによって、IPv6 クライアントをサポートします。
- FlexConnect では、IPv6 ACL、ネイバー探索キャッシュ、IPv6 NDP パケットの DHCPv6 スヌーピングはサポートされていません。
- ローカル スイッチング WLAN を使用する FlexConnect AP は、IP ソース ガードを実行して ARP スプーフィングを防ぐことはできません。中央でスイッチングされる WLAN では、ワイヤレス コントローラは IP ソース ガードおよび ARP スプーフィングを実行します。ローカル スイッチングを使用する FlexConnect AP の ARP スプーフィング攻撃を防止するために、シスコは ARP インスペクションの使用を推奨します。

Cisco Aironet Wave 2 AP でのモバイル コンシェルジュのサポート（Hotspot 2.0）

すべての Cisco Aironet Wave 2 AP で、モバイル コンシェルジュがサポートされています。

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークを接続するのに役立ちます。

ネットワークが提供するサービスは 2 つのプロトコルに分類できます。

- 802.11u MSAP
- 802.11u Hotspot 2.0

AireOS コード 8.5 以降、11ac Wave-2 AP（1800 シリーズ、2800 および 3800）で Passpoint を有効にできます。これは Wave-1 AP と同等の機能を超える、最新の Passpoint 2.0 テクノロジーへの更新です。

Cisco AP では Passpoint 認定と、AP モデル間の相互運用性が広範にサポートされています。WLC では、AireOS 8.2 コード以降 Passpoint 2.0 がサポートされており、8.5 では Wave-2 AP のサポートが追加されています。また、8.5 が動作する Mobility Express でも Passpoint 2.0 機能を使用できます。