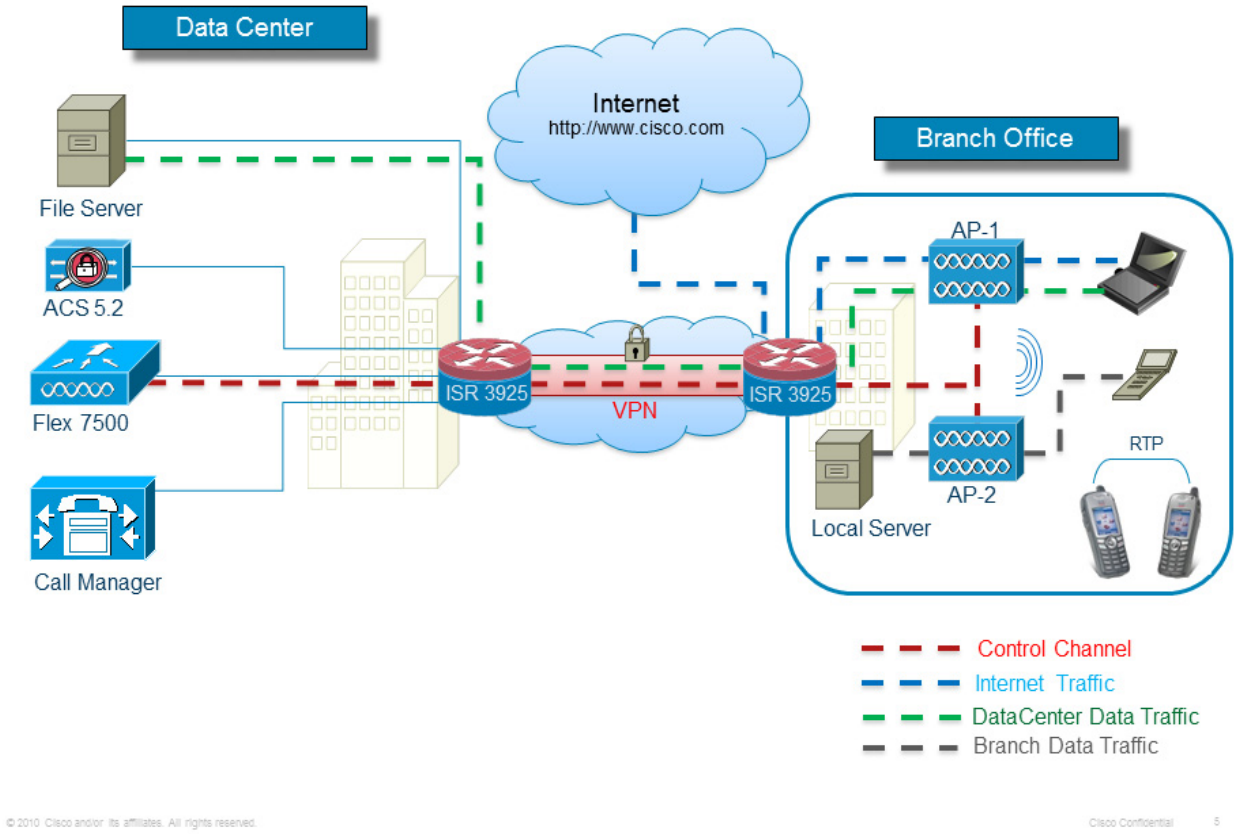
FlexConnect

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 のアクセス 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 アーキテクチャ



（注）　FlexConnect 機能マトリクスを表示するには、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。

- 1130AG、1140、1240AG、1040、1250、1260、1600、2600、3600、AP801、3500I、3500E、および AP 1260 アクセス ポイント
- Cisco Flex 7500、Cisco 8500、5500、4400、および 2500 シリーズ コントローラ
- Catalyst 3750G 統合型ワイヤレス LAN コントローラ スイッチ
- Cisco WiSM-2
- サービス統合型ルータ用のコントローラ ネットワーク モジュール
- Cisco 仮想コントローラ

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 台以上の 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を転送します。オフサイト（中央サイト）に送信されるトラフィックは、ブランチのルータによって、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、ワイヤレス アクセス ポイントのコントロールおよびプロビジョニング プロトコル（CAPWAP）経由で別々に中央集中型ワイヤレス LAN コントローラ（WLC）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、ユーザ トラフィックが WLC 上の動的インターフェイスまたは VLAN にマップされている中央集中型 WLC にトンネリングします。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ブランチ オフィスへの WAN リンクを通じて標準 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 サイトと中央サイト間の WAN リンクが停止した場合などに発生します。

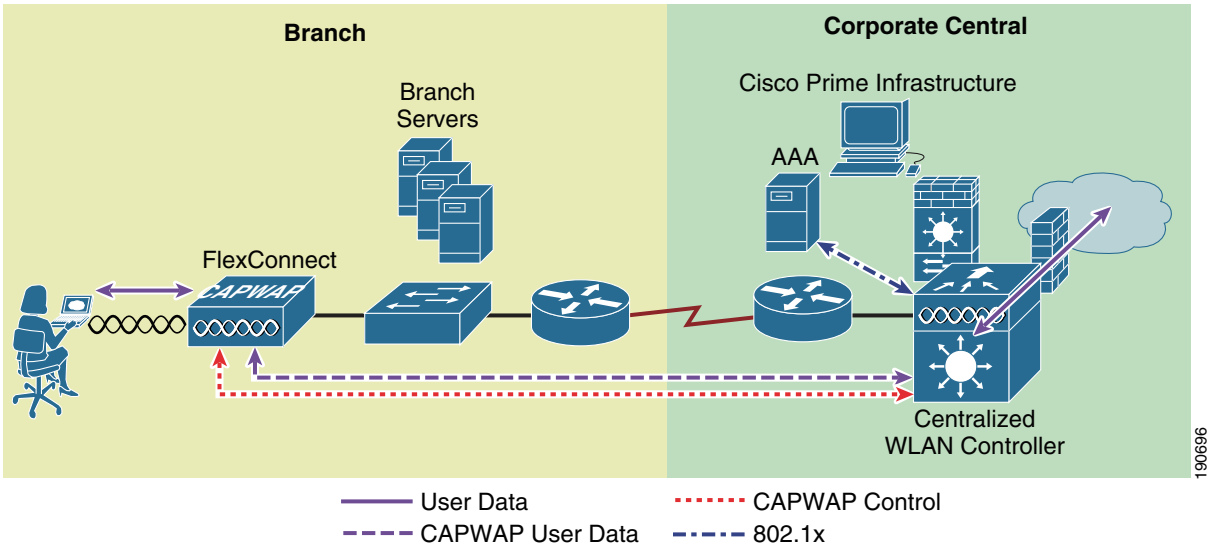
FlexConnect の状態

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



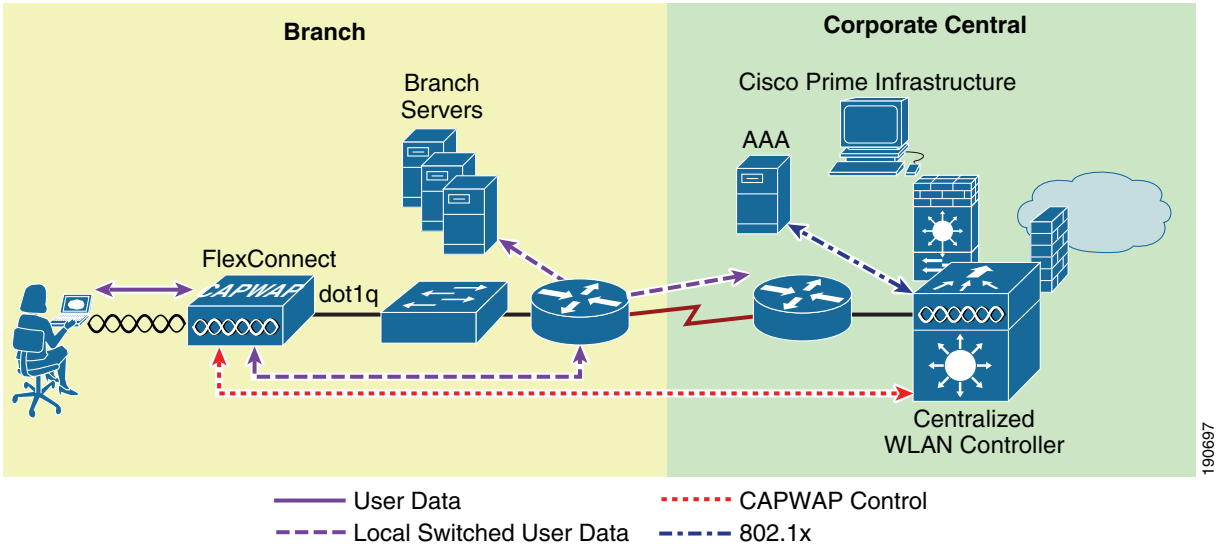
認証ダウン / スイッチング ダウン

中央スイッチング WLAN（上記）は、FlexConnect AP がスタンドアロン モードのときに、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 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。

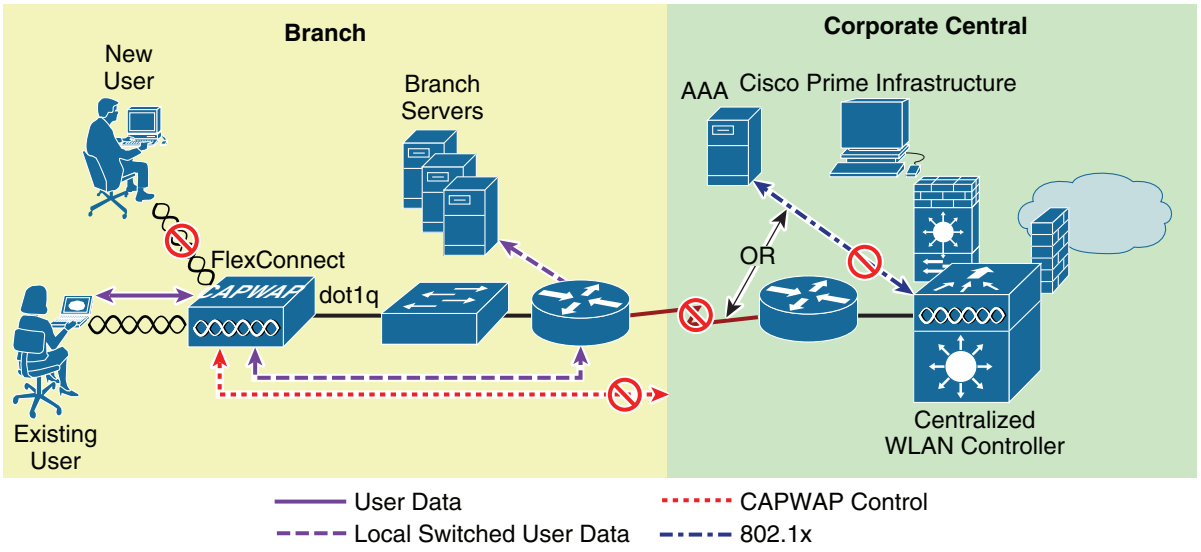
図 7-3　中央認証 / ローカル スイッチング WLAN



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）。

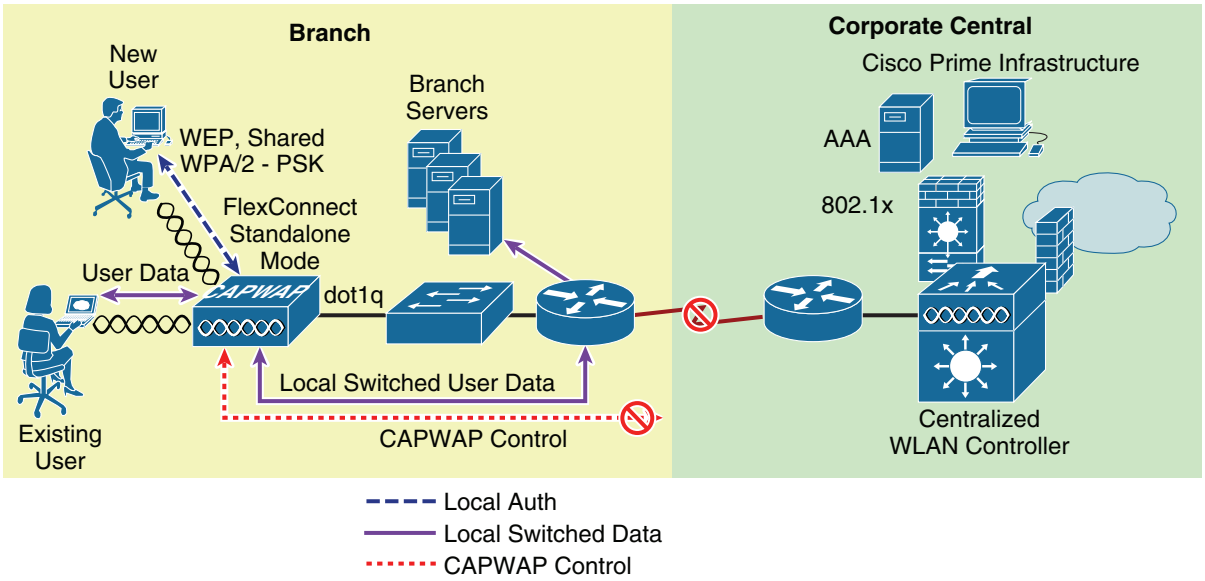
図 7-4　認証ダウン / ローカル スイッチング



ローカル認証 / ローカル スイッチング

WLAN がオープン、スタティック WEP、共有、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。これらのセキュリティ方式だけが、FlexConnect がスタンドアロン モードになったときに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 を使用することができません。

アプリケーション

FlexConnect AP は、その拡張機能によって、次のようにさらにより柔軟に展開できます。

- ブランチのワイヤレス接続
- ブランチのゲスト アクセス
- パブリック WLAN ホットスポット

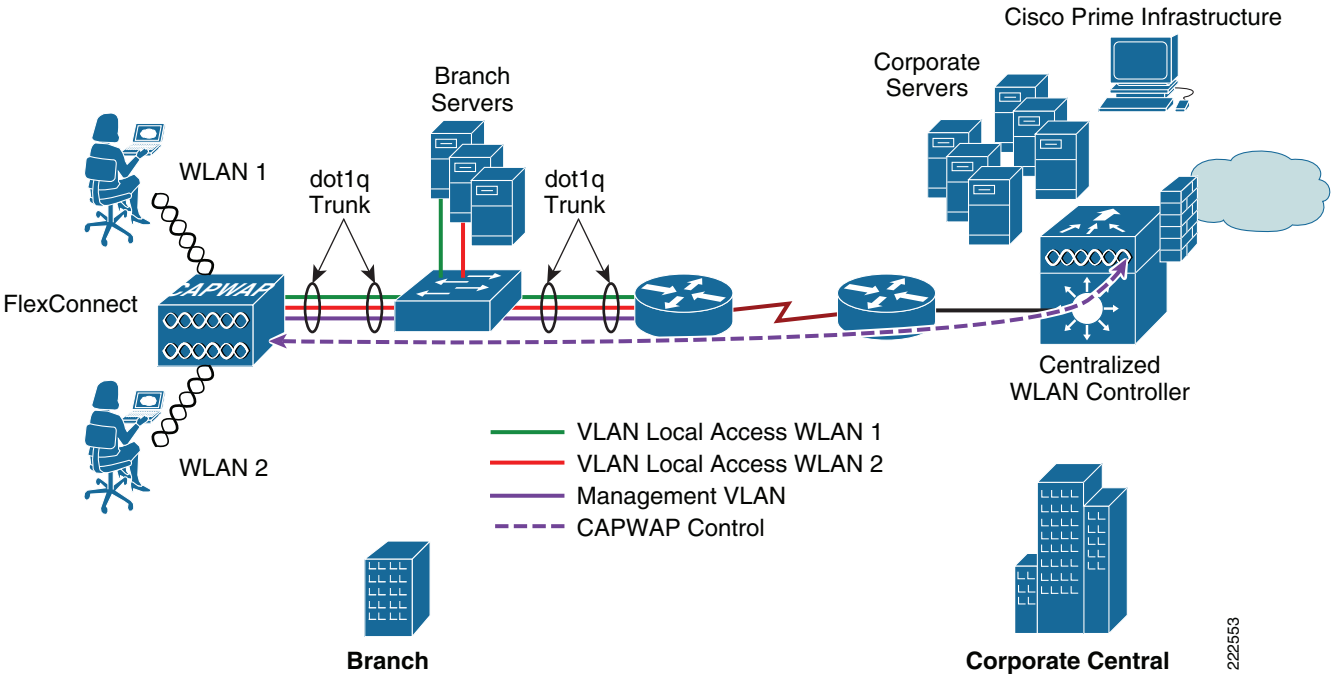
ブランチのワイヤレス接続

FlexConnect は、ワイヤレス ユーザ トラフィックを WAN を経由して中央の 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 コントロール、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 自体は、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

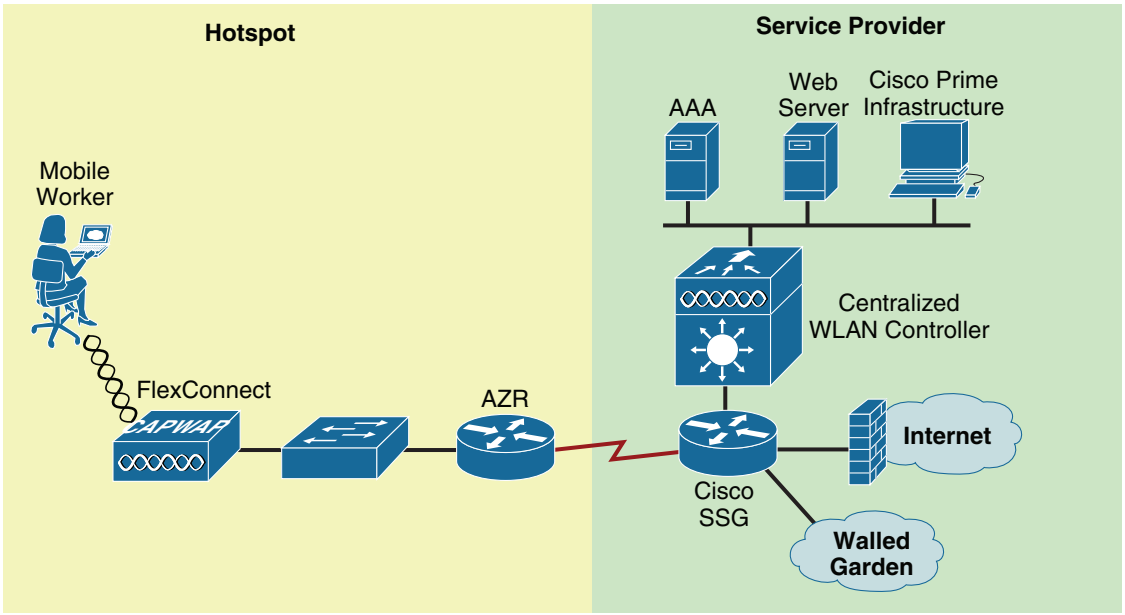


パブリック WLAN ホットスポット

多くのパブリック ホットスポット サービス プロバイダーが複数の SSID/WLAN の実装を始めています。この理由の 1 つは、オペレータが、Web ベースのアクセス用のオープンな認証 WLAN と、より安全なパブリック アクセス用に 802.1x/EAP を使用する別の WLAN を提供することを希望しているためです。

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 に取って代わっています。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



導入に関する考慮事項

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 を予想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 リンクに 100 ミリ秒を超える遅延を与えないように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、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 がスタンドアロン 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」（P.7-4）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。そうでない場合、クライアントは、認証のタイムアウトを待機することになり、それによって、ルーピングなど、その他の予測不可能な動作が発生する可能性があります。
- 帯域幅：所定のロケーションで最大 8 カ所の AP が展開されている場合は、WAN リンクは 128 kbps 以上が必要です。8 カ所を超える AP を展開する場合、比例配分により高い帯域幅が WAN リンクに提供される必要があります。
- 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、AP がスタンドアロン モードのときに、オープン、スタティック WEP および WPA PSK ベースの WLAN など、これらの認証方式を使用するために CAPWAP 接続を必要としない場合にも当てはまります。

- ダイナミック WEP/WPA：これらのキー管理方式の 1 つを使用して 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 展開と同じですが、FlexConnect トポロジ内の動作を除き、WAN 全体にわたるリンク遅延変動が生じる可能性があり、それにより合計ローミング時間に影響する可能性があります。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。

  WLAN が中央にスイッチングされるか、ローカルにスイッチングされるかに関係なく、FlexConnect は PKC をサポートしません。そのため、FlexConnect AP 間をローミングする PKC 対応クライアントは、完全な 802.1x 認証を受けることになります。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なリモート ブランチ ロケーションでは、ローカル WLC（サービス統合型ルータ用の Cisco WLC2100 または NM-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、CCKM 対応クライアントのセキュリティ資格情報は 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、その資格情報が 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。
- 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 ルータに対して 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、ローミング性能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 IP アドレスを含むように 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、送信電力制御（TPC）を行うために、最低 4 カ所の 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）トラフィックにローカルで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 タグの dot1p 値をマーク付けします。これはタグ付き VLAN でのみ発生し、ネイティブ VLAN では発生しません。

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のフレームにアソシエートされている WMM 値をキューに入れ、マーク付けします。

WLAN QoS プロファイルは、アップストリーム パケットとダウンストリーム パケットの両方に適用されます。ダウンストリームでは、デフォルト WLAN 値より高い 802.1p 値を受信した場合、デフォルト 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 WLAN 値より高い WMM 値を送信した場合、デフォルト WLAN 値が使用されます。WMM 以外のトラフィックの場合、AP からのクライアント フレームには CoS マーク付けはありません。

詳細については、第 5 章「Cisco Unified Wireless QoS」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 上で実装することを強く推奨します。適切なプライオリティ キューは、CAPWAP コントロール トラフィックのために予約して、輻輳が原因で接続モードとスタンドアロン モード間を FlexConnect AP が間違って循環しないようにする必要があります。

展開に関する一般的な考慮事項

いずれの WLC 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 合計数によって、FlexConnect AP 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 キャンパス内で AP と同じポリシーを共有せず、各ブランチ ロケーションは、基本的にそれ自体の RF およびモビリティ ドメインです。単一 WLC を複数の論理 RF およびモビリティ ドメインに分割できない場合でも、専用 WLC によって、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。

展開した場合、専用 FlexConnect WLC をメイン 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 に接続されたすべての FlexConnect AP は、その RF およびモビリティ ドメインのメンバとなります。

ここでは、auto-RF の観点から、十分な FlexConnect AP が所定のブランチ内に展開されたと想定します（「無線リソース管理」（P.7-11）を参照）。WLC は、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。

独自のモビリティ ドメインに統合された FlexConnect AP が存在しても、利点（または不都合）はありません。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、クライアントと FlexConnect AP とのローミングが発生する（同じモビリティ ドメインの）WLC 間で呼び出されません。

専用 WLC が FlexConnect 展開に使用される場合、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 LAP の展開では、指定された WLC とのアソシエーションを強制するために、WLC 優先度を H-REAP に設定する必要があります。

FlexConnect ソリューション

FlexConnect ソリューションでは、次の作業を行うことができます。

- トラフィックの中央集中型制御および管理を行う。
- 各ブランチ オフィスでクライアント データ トラフィックを配信する。
- 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する。

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単一ペイン
- 管理の容易性
- データセンターの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 トラフィックを配信する利点

クライアント データ トラフィックを配信する利点は次のとおりです。

- 完全な WAN リンクの障害発生またはコントローラの使用不能による運用上のダウンタイムなし（サバイバビリティ）。
- WAN リンクの障害発生時のブランチ内のモビリティの復元性。
- ブランチの拡張性の向上。最大 100 カ所の 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。

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非ゲスト クライアントにのみ適用される 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非ゲスト ユーザのレイヤ 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で配信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 認証	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
条件付き 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	外部	許可

Cisco Flex 7500 シリーズ Cloud Controller

Cisco Flex 7500 シリーズ Cloud Controller は、最大 500 カ所のブランチ ロケーションのワイヤレス AP を管理可能です。IT マネージャはデータセンターから、最大 3000 の AP および最大 30,000 のクライアントの設定、管理、およびトラブルシューティングを行うことができます。Cisco Flex 7500 シ

リーズ Cloud Controller は、セキュアなゲスト アクセス、Payment Card Industry（PCI）コンプライアンスのための不正検出、およびブランチ内部（ローカル スイッチング）での Wi-Fi の音声とビデオをサポートします。

Cisco Flex 7500 シリーズ Cloud Controller は、1040、1130、1140、1240、1250、1260、1550、2600、3500、3600、OEAP 600、ISR 881、および ISR 891 の各 AP をサポートします。これらの AP は複数の SSID をサポートします。

表 7-3 では、Flex 7500、WiSM WLC 2、および WLC 5500 シリーズ コントローラ間の拡張性を比較します。

表 7-3　コントローラの拡張性の比較

拡張性	Flex 7500	WiSM-2	WLC 5500
合計アクセス ポイント数	6,000	1000	500
合計クライアント数	64,000	15,000	7,000
FlexConnect の最大グループ数	2,000	100	100
FlexConnect グループあたり最大 AP 数	100	25	25
最大 AP グループ	600	1000	500

動作モード

FlexConnect には、次の 2 種類の動作モードがあります。その内容は次のとおりです。

接続済み：FlexConnect は、その CAPWAP コントロール プレーン（コントローラへの戻り）がアップ状態になっていて、動作しているときに、接続モードにあると見なされます。つまり、WAN リンクはアップ状態になり、期待どおりに動作します。

スタンドアロン：FlexConnect は、コントローラへの戻りの接続がなくなったときにスタンドアロン モードになります。スタンドアロン モードの FlexConnect AP は、電源障害や WAN 障害が発生した場合でも、直前の既知の設定によって動作し続けます。

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。ラウンドトリップ遅延が、データ展開の場合は 300 ミリ秒、データ + 音声展開の場合は 100 ミリ秒を超えない状態で、最小帯域幅の制限を AP あたり 12.8 kbps のままにすることを強く推奨します。（表 7-4 を参照）。最大伝送単位（MTU）は、少なくとも 500 バイトにする必要があります。

表 7-4　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（最大）	ブランチあたりクライアント（最大）
データ	64 kbps	300 ミリ秒	5	25
データ + 音声	128 kbps	100 ms	5	25
モニタ	64 kbps	2 秒	5	該当なし
データ	640 kbps	300 ミリ秒	50	1000

表 7-4　帯域幅の最小値 （続き）

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（最大）	ブランチあたりクライアント（最大）
データ + 音声	1.44 Mbps	100 ms	50	1000
モニタ	640 kbps	2 秒	50	該当なし

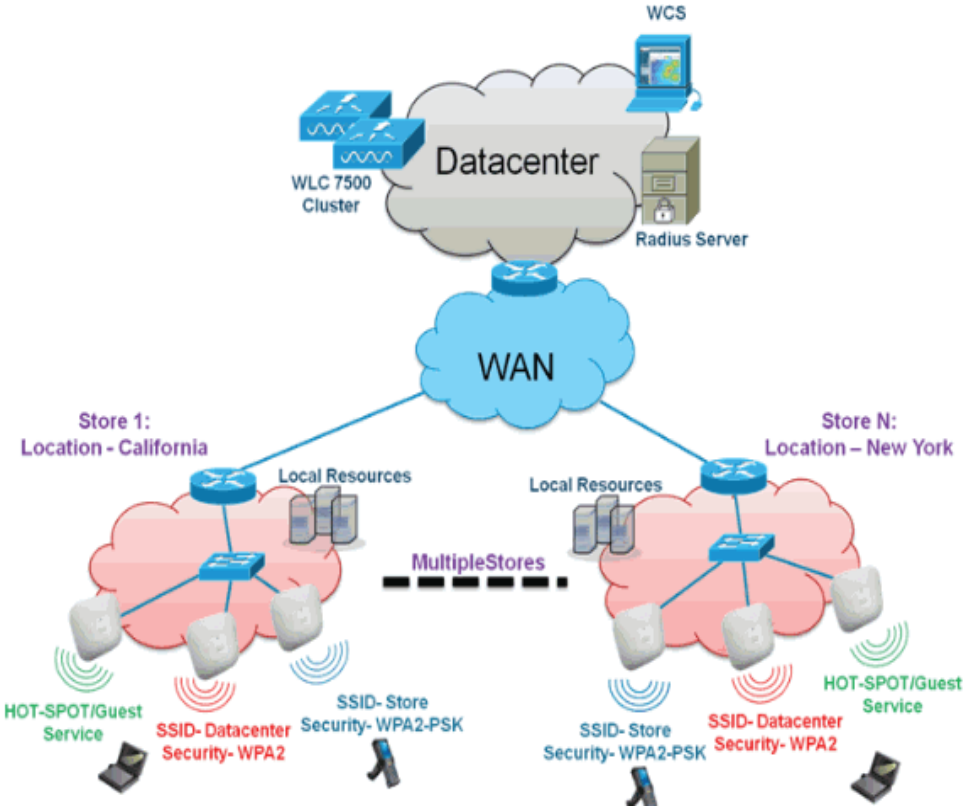
主要な設計要件は次のとおりです。

- 最大 100 カ所の 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。
- 中央集中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

ブランチ ネットワーキング機能とベスト プラクティス

FlexConnect ソリューションは、データセンター内の複雑なセキュリティ、管理、設定、トラブルシューティング処理を仮想化し、これらのサービスを各ブランチに透過的に拡張します。FlexConnect コントローラを使用した展開では、IT の設定、管理がより簡単になりますが、最も重要なことは拡大縮小がより簡単になることです（図 7-8 を参照）。

図 7-8　ワイヤレス ブランチ ネットワークの設計



次の機能とベスト プラクティスが含まれています。

- FlexConnect グループ：ローカル バックアップ Radius、Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミング、ローカル認証の機能を提供します。
- 耐障害性：ワイヤレス ブランチの復元力を高め、運用上のダウンタイムをなくします。
- ELM（Adaptive wIPS 用の拡張ローカル モード）：クライアントにサービスを提供するときに、クライアントのパフォーマンスに影響を与えることなく、Adaptive wIPS 機能を提供します。
- WLAN ごとのクライアント制限：ブランチ ネットワーク上のゲスト クライアントの総数を制限します。
- FlexConnect における AP の自動変換：ブランチの FlexConnect の AP を自動的に変換するための機能。
- ゲスト アクセス：シスコの既存のゲスト アクセス アーキテクチャを FlexConnect で引き続き使用できます。

FlexConnect グループ

各ブランチ サイトの FlexConnect AP は、すべて単一の FlexConnect グループの一部であるため、FlexConnect グループは各ブランチ サイトの構成を簡素化します。

（注）　FlexConnect グループは AP グループに類似していません。

FlexConnect グループは、主に次の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、またはプライマリおよびセカンダリ 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。

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 Store 1 を割り当てます（図 7-8 に示す設定と同様です）。

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。

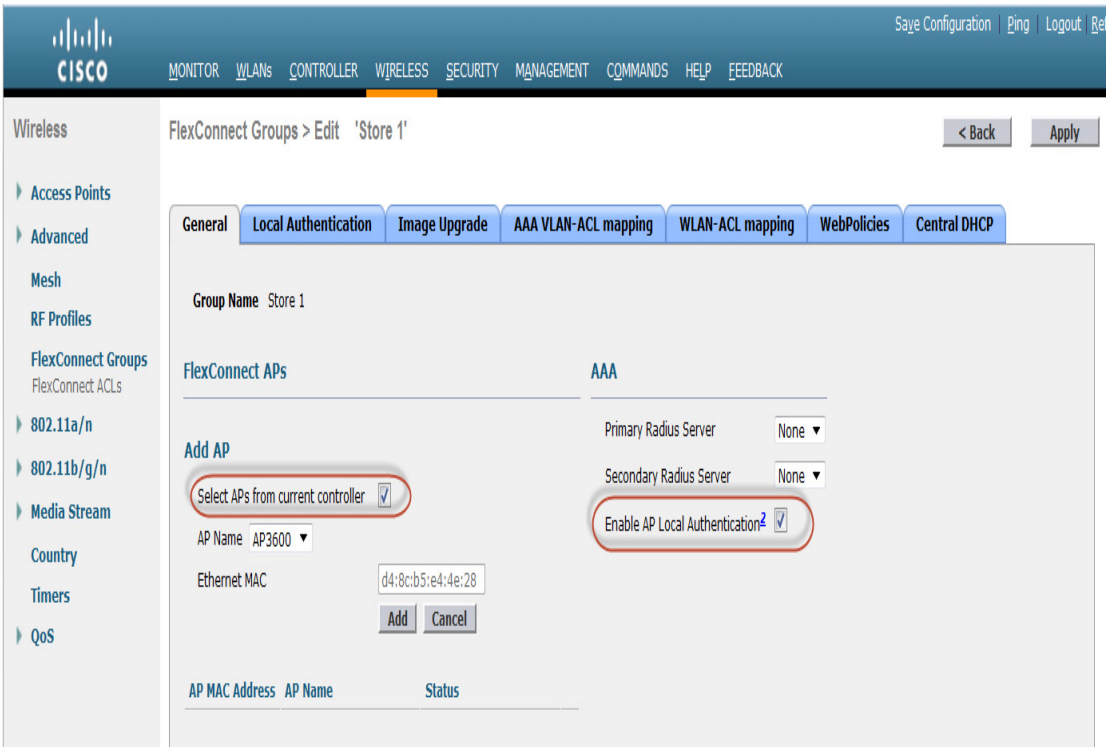
ステップ 5　[Add AP] をクリックします。

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イネーブルにするには、[Enable AP Local Authentication] 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 メニューをイネーブルにするには、[Select APs from current controller] 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 をドロップダウンから選択します。

ステップ 9　AP をドロップダウンから選択した後、[Add] をクリックします。



ステップ 10　ステップ 7 と 8 を繰り返し、この FlexConnect グループ Store 1 にすべての 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] タブ、[Protocols] タブを順にクリックして、[Enable LEAP Authentication] ボックスをオンにします。

ステップ 12　チェックボックスを設定した後、[Apply] をクリックします。

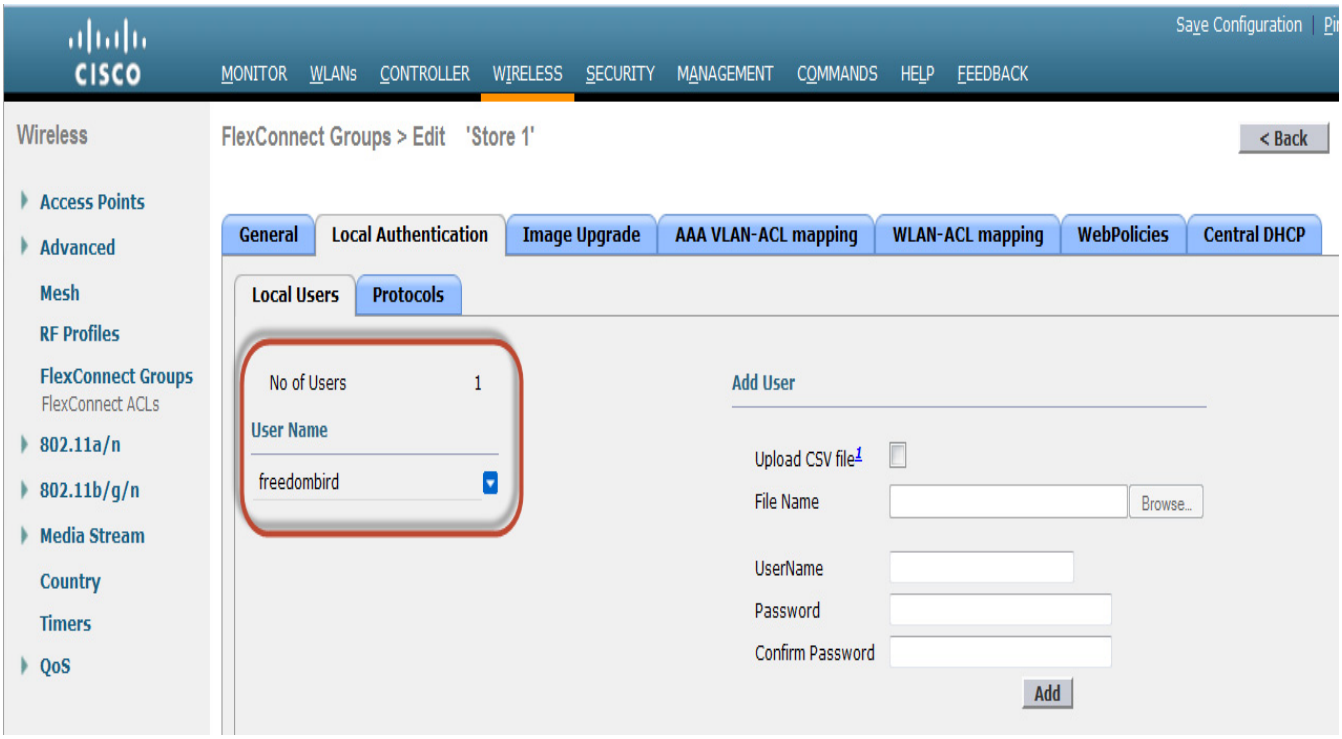
（注）　バックアップ コントローラがある場合は、FlexConnect グループごとに、FlexConnect グループが同じであり、AP の MAC アドレス エントリが含まれていることを確認します。

ステップ 13　[Local Authentication] の [Local Users] をクリックします。

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　ローカル ユーザ名リストがなくなるまでステップ 13 を繰り返します。100 人を超えるユーザの設定や追加はできません。

ステップ 16　ローカル ユーザ情報の入力がすべて完了したら [Apply] をクリックします。ユーザの数を確認します。

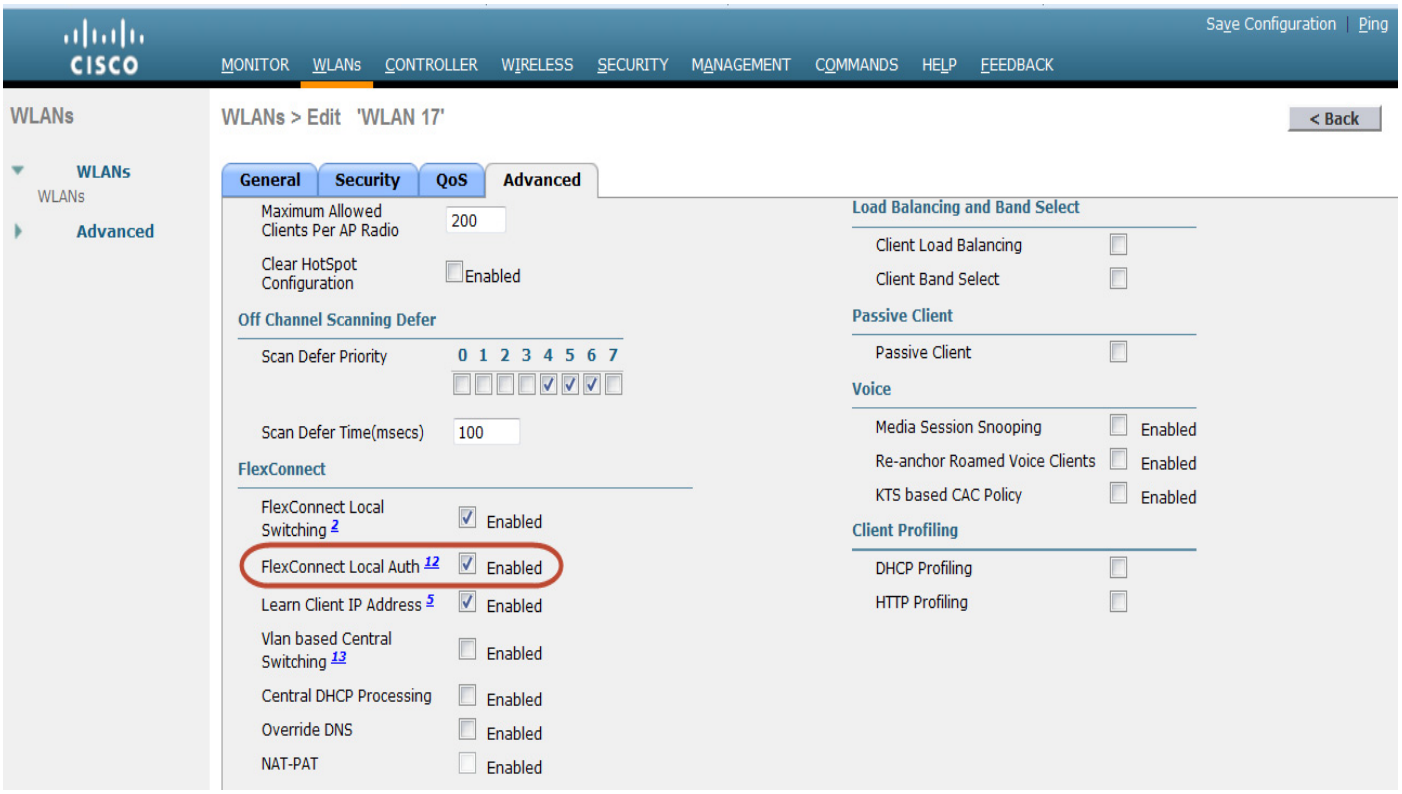


ステップ 17　上部のペインで [WLANs] をクリックします。

ステップ 18　AP グループの作成時に作成された [WLAN ID] の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] の下で、[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イネーブルにするには、[FlexConnect Local Auth] 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した FlexConnect のみでサポートされます。WLAN の下でローカル認証をイネーブルにする前に、必ず FlexConnect グループを作成してください。

CLI を使用した確認

クライアント認証状態とスイッチング モードは、WLC 上で次の CLI コマンドを使用してすばやく確認できます。

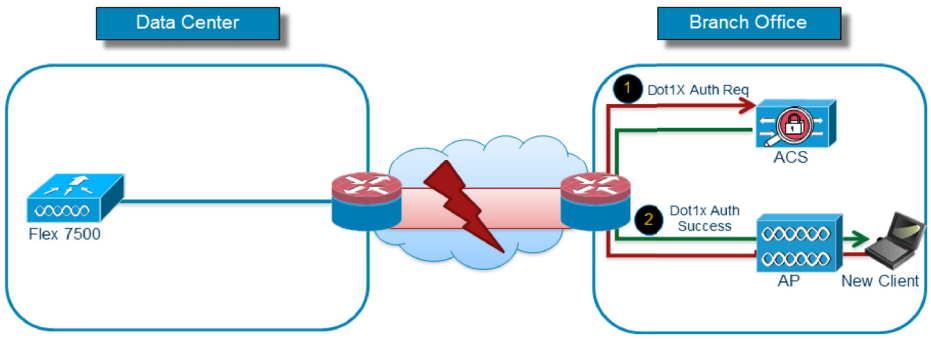
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
    Client MAC Address.............................00:24:d7:2b:7c:0c
    Client Username................................N/A
    AP MAC Address.................................d0:57:4c:08:e6:70
    Client State...................................Associated
    FlexConnect Data Switching.....................Local
    FlexConnect Authentication.....................Local
```

ローカル認証

図 7-9 に示すように、FlexConnect ブランチ AP がコントローラに接続できない場合でも、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。

言い換えれば、RADIUS/ACS がブランチの中にある場合、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。

図 7-9　　ローカル認証：AP オーセンティケータ



（注）　この機能は、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 グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、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。その後、セカンダリ バックアップ RADIUS サーバを試行し（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。コントローラは、それぞれの FlexConnect アクセス ポイントがコントローラに join すると、ユーザ名とパスワードのスタティック リストをその特定の FlexConnect グループの FlexConnect AP に送信します。グループ内の各 AP は、そのアクセス ポイント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際に別のハードウェア デバイスを追加したくない場合です。

CCKM/OKC 高速ローミング

FlexConnect グループは、FlexConnect AP と共に使用する Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミングで必要となります。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 AP 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。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。

たとえば、300 個の 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して 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。限定されたいくつかの AP からなる FlexConnect グループを作成すれば（たとえば、同じリモート オフィス内の 4 個の AP のグループを作成）、クライアントはその 4 個のアクセス 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 個の AP 間で配布されるのは、クライアントが 1 個の AP 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。

（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あるため、FlexConnect AP 上で特定の WLAN にアソシエーションされたクライアントは、それ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 にアソシエーションする必要があるので、さまざまな制約があります。

7.2 リリースより、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、個別の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、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。WLC は、AP でサブインターフェイスを事前作成するために使用されます。

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 について、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 上でイネーブルにする必要があります。
- FlexConnect AP には、ダイナミック 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 から、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（ダイナミック VLAN 割り当て）により、ワイヤレス クライアントが AAA サーバで提供される VLAN に配置されます。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 からマッピングされた VLAN に配置され、トラフィックはその VLAN 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、VLAN が WLC 上に存在する限り、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。

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 コントロールの必要性を満たすメカニズムがあります。FlexConnect ACL を WLC 上で作成し、FlexConnect AP か、AAA オーバーライド VLAN 用の VLAN-ACL マッピングを使用した FlexConnect グループ上に存在する VLAN を使用して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

- コントローラで FlexConnect ACL を作成します。
- 同じことを、AP レベル VLAN ACL マッピングの下で、FlexConnect AP 上に存在する VLAN に適用します。
- VLAN-ACL マッピングの下で、FlexConnect グループに存在する VLAN に適用できます（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

- 最大 512 個の FlexConnect ACL を WLC に対して設定できます。
- 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。
- 最大 16 個の VLAN と 32 個の ACL が FlexConnect AP 上に同時に存在できます。

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、残りのパケットは 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 AP 構成に対するさらなるメリットがあります。

FlexConnect ACL は、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するために、ルールを使用して作成できます。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、残りのトラフィック（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、中央サイトのクライアントにアソシエーションされているサブネットまたは VLAN がローカル サイトに存在しないことを前提としています（つまり、中央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 トンネリング機能は、WAN の帯域幅の使用を避けるために、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ています。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、NAT 操作が実行され、クライアントの送信元 IP アドレスが、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。
- 必要な DHCP を、スプリット トンネリングが設定された WLAN 上でイネーブルに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 ごとか、FlexConnect グループ内のすべての FlexConnect AP に対して、中央の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、これらの設定された WLAN 上のワイヤレス クライアントに送信された場合、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。

耐障害性

FlexConnect の耐障害性を使用すると、FlexConnect AP で次の状態が生じたときに、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です。

- 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 コントローラに切替えるとき。
- プライマリ コントローラとの接続を再確立するとき。

FlexConnect の耐障害性は、ローカル EAP と共に、ネットワーク停止時のゼロ ブランチ ダウンタイムを提供します。この機能はデフォルトでイネーブルになっており、ディセーブルにできません。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

- FlexConnect は、コントローラの設定が変更されない限り、AP が同じコントローラに接続するときにクライアントを切断しません。
- FlexConnect は、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、バックアップ コントローラに接続するときにクライアントを切断しません。
- FlexConnect は、コントローラの設定に変更がない限り、プライマリ コントローラに接続するときに、その無線をリセットしません。

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した FlexConnect のみでサポートされます。
- 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、中央で認証されるクライアントの完全な再認証が必要です。
- 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 ブロック

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。

- [Disabled] : P2P ブロッキングをディセーブルにし、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。
- [Drop] : 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ドロップします。
- [Forward Up-Stream] : 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 上でドロップまたはアップストリーム転送として設定された P2P ブロッキング アクションは、FlexConnect AP でイネーブルにされた P2P ブロッキングとして扱われます。

P2P の制限事項

- FlexConnect では、ソリューション P2P ブロッキング設定を特定の FlexConnect AP または AP のサブセットのみに適用できません。
- 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 にアソシエーション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。FlexConnect ACL は、この制限の回避策として使用できます。

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 はその各有線またはワイヤレス クライアントについて IAPP メッセージを送信し、Flex 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、Flex AP からローカルにスイッチングされます。
- AP がスタンドアロン モードの場合、AP が IAPP メッセージを処理し、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、接続モードに遷移するときに、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遷移するとき、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。WGB の背後にあるクライアントに対する複数 VLAN のサポートは、ローカル スイッチングが設定された WLAN について、FlexConnect AP 上でサポートされていません。
- 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。

注意事項と制約事項

- 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。
- CAPWAP コントロール パケットは、他のすべてのトラフィックに優先する必要があります。
- 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が 300 ミリ秒を達成できない場合は、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含まれています。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、クライアントはシームレスな接続が行われます。
- 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後、AP の無線もリセットされます。
- 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、スタティック 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。
- コントローラの設定は、AP がスタンドアロン モードに移行し、接続モードに戻るまでの時間、変更*しないでください*。同様に、AP がセカンダリ コントローラまたはバックアップ コントローラにフォール バックする場合、プライマリ コントローラとセカンダリ コントローラまたはバックアップ コントローラ間の設定は変更しないでください。
- 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、電流 / サポート 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。
- コントローラは、ユニキャスト パケットまたはマルチキャスト パケットの形式でマルチキャスト パケットを AP に送信できます。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 で CCKM 高速ローミングを使用するには、FlexConnect グループを設定する必要があります。
- 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。
- QoS ユーザ単位帯域幅コントラクトは、ローカル モードの中央スイッチング WLAN および AP でのみサポートされます。QoS プロファイルのユーザ単位帯域幅コントラクトは、FlexConnect ローカル スイッチング WLAN ではサポート*されません*。
- ゲスト ユーザ設定は、FlexConnect ローカル スイッチングではサポートされていません。
- 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 ディスカバリ キャッシュ、または 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。